

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant: Masanao SAKAI

Title: NETWORK, IPsec SETTING SERVER APPARATUS, IPsec PROCESSING APPARATUS, AND IPsec SETTING METHOD USED THEREFOR

Appl. No.: Unassigned

Filing Date: 09/05/2003

Examiner: Unassigned

Art Unit: Unassigned

CLAIM FOR CONVENTION PRIORITY

Commissioner for Patents
PO Box 1450
Alexandria, Virginia 22313-1450

Sir:

The benefit of the filing date of the following prior foreign application filed in the following foreign country is hereby requested, and the right of priority provided in 35 U.S.C. § 119 is hereby claimed.

In support of this claim, filed herewith is a certified copy of said original foreign application:

Japanese Patent Application No. 2002-264913
filed 09/11/2002.

Respectfully submitted,

Michael M. Blumenthal

Reg. No. 34,717

By _____

fb David A. Blumenthal
Attorney for Applicant
Registration No. 26,257

Date: September 5, 2003

FOLEY & LARDNER
Customer Number: 22428



22428

PATENT TRADEMARK OFFICE

Telephone: (202) 672-5407

Facsimile: (202) 672-5399

日本国特許庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日 2002年 9月11日
Date of Application:

出願番号 特願2002-264913
Application Number:

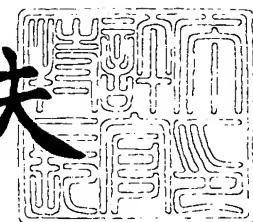
[ST. 10/C] : [JP2002-264913]

出願人 日本電気株式会社
Applicant(s):

2003年 8月12日

特許庁長官
Commissioner,
Japan Patent Office

今井康夫



【書類名】 特許願

【整理番号】 41810227

【提出日】 平成14年 9月11日

【あて先】 特許庁長官殿

【国際特許分類】 H04L 9/00

【発明者】

【住所又は居所】 東京都港区芝五丁目 7番1号 日本電気株式会社内

【氏名】 酒井 征直

【特許出願人】

【識別番号】 000004237

【氏名又は名称】 日本電気株式会社

【代理人】

【識別番号】 100088812

【弁理士】

【氏名又は名称】 ▲柳▼川 信

【手数料の表示】

【予納台帳番号】 030982

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9001833

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 ネットワーク、IPsec設定サーバ装置、IPsec処理装置及びそれらに用いるIPsec設定方法

【特許請求の範囲】

【請求項1】 異なる2つの拠点間をインターネットを介して通信する場合にインターネット経路上でのセキュリティを確保するためのIPsec (Internet Protocol security protocol) を使用するIPsec処理装置と、前記IPsec処理装置のIPsec設定を管理するIPsec設定サーバ装置とを含むネットワークであって、第1及び第2のIPsec処理装置間に適用する前記IPsecのポリシーを一括管理する機能を前記IPsec設定サーバ装置に有することを特徴とするネットワーク。

【請求項2】 前記第1のIPsec処理装置から受信した前記第2のIPsec処理装置との間の通信に対する要求メッセージの内容を基に前記第2のIPsec処理装置との間に適用する前記IPsecのポリシーを特定する機能を前記IPsec設定サーバ装置に含むことを特徴とする請求項1記載のネットワーク。

【請求項3】 前記要求メッセージを受信した場合に当該要求メッセージを送信した前記第1のIPsec処理装置の通信相手である前記第2のIPsec処理装置に対して当該通信用の要求メッセージを送信させるために要求起動メッセージを送信する機能を前記IPsec設定サーバ装置に含むことを特徴とする請求項2記載のネットワーク。

【請求項4】 前記要求起動メッセージに対する応答がない時に前記第1のIPsec処理装置に対して前記第2のIPsec処理装置からの応答なしを通知する機能を前記IPsec設定サーバ装置に含むことを特徴とする請求項3記載のネットワーク。

【請求項5】 前記要求メッセージの内容とそれに適用する前記IPsecのポリシーの内容とから当該IPsec通信に必要となるSA (Security Association) パラメータを生成する機能を前記IPsec設定

サーバ装置に含むことを特徴とする請求項2から請求項4のいずれか記載のネットワーク。

【請求項6】 前記要求メッセージに対して前記IPsecのポリシーと前記SAパラメータとを少なくとも含む配布メッセージを送信する機能を前記IPsec設定サーバ装置に含むことを特徴とする請求項2から請求項5のいずれか記載のネットワーク。

【請求項7】 前記IPsecの暗号化及び認証に使用するための共有秘密鍵を生成する機能と、その生成した前記共有秘密鍵を前記IPsec処理装置に配布する機能とを前記IPsec設定サーバ装置に含むことを特徴とする請求項1から請求項6のいずれか記載のネットワーク。

【請求項8】 異なる2つの拠点間をインターネットを介して通信する場合にインターネット経路上でのセキュリティを確保するためのIPsec (Internet Protocol security protocol) を使用するIPsec処理装置のIPsec設定を管理するIPsec設定サーバ装置であって、前記IPsec処理装置間に適用する前記IPsecのポリシーを一括管理する機能を有することを特徴とするIPsec設定サーバ装置。

【請求項9】 前記IPsec処理装置から受信した他のIPsec処理装置との間の通信に対する要求メッセージの内容を基に前記他のIPsec処理装置との間に適用する前記IPsecのポリシーを特定する機能を含むことを特徴とする請求項8記載のIPsec設定サーバ装置。

【請求項10】 前記要求メッセージを受信した場合に当該要求メッセージを送信したIPsec処理装置の通信相手のIPsec処理装置に対して当該信用の要求メッセージを送信させるために要求起動メッセージを送信する機能を含むことを特徴とする請求項9記載のIPsec設定サーバ装置。

【請求項11】 前記要求起動メッセージに対する応答がない時に前記要求メッセージを送信したIPsec処理装置に対して前記通信相手のIPsec処理装置からの応答なしを通知する機能を含むことを特徴とする請求項10記載の前記IPsec設定サーバ装置。

【請求項12】 前記要求メッセージの内容とそれに適用する前記IPse

c のポリシーの内容とから当該 I P s e c 通信に必要となる SA (S e c u r i t y A s s o c i a t i o n) パラメータを生成する機能を含むことを特徴とする請求項 9 から請求項 11 のいずれか記載の I P s e c 設定サーバ装置。

【請求項 13】 前記要求メッセージに対して前記 I P s e c のポリシーと前記 SA パラメータとを少なくとも含む配布メッセージを送信する機能を含むことを特徴とする請求項 9 から請求項 12 のいずれか記載の I P s e c 設定サーバ装置。

【請求項 14】 前記 I P s e c の暗号化や認証に使用するための共有秘密鍵を生成する機能と、その生成した前記共有秘密鍵を前記 I P s e c 処理装置に配布する機能とを含むことを特徴とする請求項 8 から請求項 13 のいずれか記載の I P s e c 設定サーバ装置。

【請求項 15】 インタネットにおいて I P s e c (I n t e r n e t P r o t o c o l s e c u r i t y p r o t o c o l) を使用する I P s e c 処理装置であって、前記 I P s e c を適用すべきパケットを受信した場合に I P s e c 設定サーバ装置で一括管理される当該 I P s e c に関する設定を前記 I P s e c 設定サーバ装置に問い合わせるか否かを判断する機能を有することを特徴とする I P s e c 処理装置。

【請求項 16】 前記 I P s e c に関する設定を取得するために前記 I P s e c 設定サーバ装置に他の I P s e c 処理装置との間の通信に対する要求メッセージを送信する機能を含むことを特徴とする請求項 15 記載の I P s e c 処理装置。

【請求項 17】 前記 I P s e c 設定サーバ装置から前記要求メッセージを送信させるための要求起動メッセージを受信した時に当該要求メッセージの送信を行うことを特徴とする請求項 16 記載の I P s e c 処理装置。

【請求項 18】 前記 I P s e c 設定サーバ装置から受信した配布メッセージを基に前記 I P s e c を適用するためのポリシーを記録する S P D 及び個々の通信に対して前記 I P s e c の処理を実施するために必要な SA (S e c u r i t y A s s o c i a t i o n) を記録する S A D を設定する機能を含むことを特徴とする請求項 15 から請求項 17 のいずれか記載の I P s e c 処理装置。

【請求項19】 前記IPsecの暗号化や認証に使用するための共有秘密鍵を前記IPsec設定サーバ装置から取得する機能を含むことを特徴とする請求項15から請求項18のいずれか記載のIPsec処理装置。

【請求項20】 前記SAの有効期限が満了する前に前記IPsec設定サーバ装置に前記要求メッセージを再送信して新しい設定情報を取得する機能を含むことを特徴とする請求項15から請求項19のいずれか記載のIPsec処理装置。

【請求項21】 異なる2つの拠点間をインターネットを介して通信する場合にインターネット経路上でのセキュリティを確保するためのIPsec (Internet Protocol security protocol) を使用するIPsec処理装置と、前記IPsec処理装置のIPsec設定を管理するIPsec設定サーバ装置とからなるネットワークのIPsec設定方法であって、前記IPsec処理装置間に適用する前記IPsecのポリシーを一括管理するステップを前記IPsec設定サーバ装置に有することを特徴とするIPsec設定方法。

【請求項22】 前記IPsec処理装置から受信した他のIPsec処理装置との間の通信に対する要求メッセージの内容を基に前記他のIPsec処理装置との間に適用する前記IPsecのポリシーを特定するステップを前記IPsec設定サーバ装置に含むことを特徴とする請求項21記載のIPsec設定方法。

【請求項23】 前記要求メッセージを受信した場合に当該要求メッセージを送信したIPsec処理装置の通信相手のIPsec処理装置に対して当該信用の要求メッセージを送信させるために要求起動メッセージを送信するステップを前記IPsec設定サーバ装置に含むことを特徴とする請求項22記載のIPsec設定方法。

【請求項24】 前記要求起動メッセージに対する応答がない時に前記要求メッセージを送信したIPsec処理装置に対して前記通信相手のIPsec処理装置からの応答なしを通知する機能を前記IPsec設定サーバ装置に含むことを特徴とする請求項23記載のIPsec設定方法。

【請求項25】 前記要求メッセージの内容とそれに適用する前記IPsecのポリシーの内容とから当該IPsec通信に必要となるSA（Security Association）パラメータを生成するステップを前記IPsec設定サーバ装置に含むことを特徴とする請求項22または請求項24記載のIPsec設定方法。

【請求項26】 前記要求メッセージに対して前記IPsecのポリシーと前記SAパラメータとを少なくとも含む配布メッセージを送信するステップを前記IPsec設定サーバ装置に含むことを特徴とする請求項22から請求項25のいずれか記載のIPsec設定方法。

【請求項27】 前記IPsecの暗号化や認証に使用するための共有秘密鍵を生成するステップと、その生成した前記共有秘密鍵を前記IPsec処理装置に配布するステップとを前記IPsec設定サーバ装置に含むことを特徴とする請求項21から請求項26のいずれか記載のIPsec設定方法。

【請求項28】 前記IPsec処理装置が、前記IPsecを適用すべきパケットを受信した場合にIPsec設定サーバ装置で一括管理される当該IPsecに関する設定を前記IPsec設定サーバ装置に問い合わせるか否かを判断することを特徴とする請求項21から請求項27のいずれか記載のIPsec設定方法。

【請求項29】 前記IPsec処理装置が、前記IPsecに関する設定を取得するために前記IPsec設定サーバ装置に他のIPsec処理装置との間の通信に対する要求メッセージを送信することを特徴とする請求項21から請求項28のいずれか記載のIPsec設定方法。

【請求項30】 前記IPsec処理装置が、前記IPsec設定サーバ装置から受信した配布メッセージを基に前記IPsecを適用するためのポリシーを記録するSPD及び個々の通信に対して前記IPsecの処理を実施するため必要なSA（Security Association）を記録するSADを設定することを特徴とする請求項21から請求項29のいずれか記載のIPsec設定方法。

【請求項31】 前記IPsec処理装置が、前記IPsecの暗号化や認

証に使用するための共有秘密鍵を前記IPsec設定サーバ装置から取得することを特徴とする請求項21から請求項30のいずれか記載のIPsec設定方法。

【請求項32】 前記IPsec処理装置が、前記SAの有効期限が満了する前に前記IPsec設定サーバ装置に前記要求メッセージを再送信して新しい設定情報を取得することを特徴とする請求項21から請求項31のいずれか記載のIPsec設定方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明はネットワーク、IPsec設定サーバ装置、IPsec処理装置及びそれらに用いるIPsec設定方法に関し、特にインターネット上で機密性、完全性、認証等の機能を提供するIPsec(Internet Protocol security protocol)によるネットワーク構成に関する。

【0002】

【従来の技術】

従来、インターネットの普及に伴って、インターネット上のセキュリティを確保したいという要望が高まっている。特に、多くの企業においては、高価な専用線を用いてネットワークを構築する代わりに、インターネット上に仮想的な私設網を構築し、遠隔地のオフィス等を結ぶネットワークを安価に構築したいという要望も多い。

【0003】

このような要望に対して、インターネット上で機密性、完全性、認証等の機能を提供するIPsec(Internet Protocol security protocol)がIETF(Internet Engineering Task Force)によって標準化されている(例えば、特許文献1参照)。

【0004】

IPsecを用いることによって、異なる2つの拠点間をインターネットを介し

て通信する場合には、インターネット経路上でのセキュリティを確保することが可能となる。新しいインターネットプロトコルであるIPv6 (Internet Protocol version 6) ではIPsecのサポートが必須となり、今後、ますます多くのネットワーク機器がIPsecに対応し、IPsecを使用した通信もますます増えることが予想される。

【0005】

このIPsecを使用した通信を行うIPsec処理装置の構成を図31に示す。図31において、IPsec処理装置4はインターフェース部(I/F)41, 42と、IPsec処理部43と、SPD(Security Policy Database)44と、SAD(Security Association Database)45と、ルーティング部46とを具備している。

【0006】

インターフェース部41はプライベートネットワークに接続され、プライベートネットワークとのデータ通信を行う。インターフェース部42はインターネットに接続され、インターネットを介したデータ通信を行う。

【0007】

IPsec処理部43はインターフェース部41, 42から受信したデータ通信パケットに対してIPsec処理を実施する。SPD44はIPsec処理部43から参照され、IPsecを適用するためのポリシーが記録されている。SAD45はIPsec処理部43から参照され、個々の通信に対してIPsec処理を実施するために必要なSAが記録されている。ルーティング部46はIPsec処理部43との間でデータ通信パケットの送受信を行い、各々のデータ通信パケットの転送先を決定する。

【0008】

特開2001-298449号公報(第8-11頁、図1)

【0009】

【発明が解決しようとする課題】

しかしながら、上述した従来のIPsecによるネットワーク構成では、1台のIPsec処理装置が多くの相手とIPsec通信を実施する場合、IPse

cによる接続において、IPsec処理を実施する装置に設定する内容が多いという問題がある。

【0010】

IPsecを利用するためには、IPsecを適用する通信に対して使用するサービス[AH (A u t h e n t i c a t i o n H e a d e r : 認証ヘッダ) , ESP (E n c a p s u l a t i n g S e c u r i t y P a y l o a d : カプセル化セキュリティペイロード) によって提供されるサービス]、使用するアルゴリズム等を、IPsec処理を実施する両端の装置にそれぞれ設定する必要がある。

【0011】

自動鍵管理プロトコル (IKE : I n t e r n e t K e y E x c h a n g e) を使用する場合には、自動鍵管理プロトコルで利用される暗号化アルゴリズム、ハッシュアルゴリズム、鍵共有アルゴリズム等も両端の装置に設定する必要がある。これらの設定の数はIPsecによって接続する相手毎に必要となるため、IPsecによって接続する相手が多くなるほど、多くの設定が必要となる。

【0012】

また、従来のIPsecによるネットワーク構成では、IPsecを適用する通信の両端で異なる設定をしてしまう可能性があるという問題がある。IPsec処理を実施する両端の装置において、使用するサービスの設定や、使用するアルゴリズムの設定に異なる設定をしてしまった場合、通信することができなくなる。IPsecを適用する通信が多くなると、設定の数も多くなるため、このような間違いが発生する可能性も増える。

【0013】

さらに、従来のIPsecによるネットワーク構成では、自動鍵管理プロトコルを使用した場合に、共有秘密鍵を生成する演算に時間がかかり、結果として通信を開始することができるまでに時間がかかるという問題がある。通常、IPsec処理装置では、図32に示すように、当該通信が必要になった時点で初めて共有秘密鍵の生成を始めるため、共有秘密鍵の生成に時間がかかるれば、通信開

始までに時間がかかるてしまう。

【0014】

さらにまた、従来のIPsecによるネットワーク構成では、自動鍵管理プロトコルを使用した場合に、IPsec処理を実施する装置に演算負荷が発生するという問題がある。共有秘密鍵を生成するためには多くの演算が必要となり、当該装置の持つ他の機能（IPsecを適用しないパケットの転送機能等）の性能が低下してしまう。同時に扱うIPsec通信が多くなると、共有秘密鍵を生成する機会も多くなり、性能が低下する割合も多くなる。

【0015】

そこで、本発明の目的は上記の問題点を解消し、通信する装置間での設定不一致を防止することができるネットワーク、IPsec設定サーバ装置、IPsec処理装置及びそれらに用いるIPsec設定方法を提供することにある。

【0016】

また、本発明の他の目的は、ポリシー設定後の暗号化や復号を滞りなく行うことができ、送信元からのパケットを取りこぼしなく受取ることができるネットワーク、IPsec設定サーバ装置、IPsec処理装置及びそれらに用いるIPsec設定方法を提供することにある。

【0017】

また、本発明の別の目的は、秘密鍵演算を不要とし、個々の装置での通信開始時のIPsec経路の接続時間を短縮することができ、性能の低下を防ぐことができるネットワーク、IPsec設定サーバ装置、IPsec処理装置及びそれらに用いるIPsec設定方法を提供することにある。

【0018】

【課題を解決するための手段】

本発明によるネットワークは、異なる2つの拠点間をインターネットを介して通信する場合にインターネット経路上でのセキュリティを確保するためのIPsec（Internet Protocol security protocol）を使用するIPsec処理装置と、前記IPsec処理装置のIPsec設定を管理するIPsec設定サーバ装置とを含むネットワークであって、前記IP

s e c 处理装置間に適用する前記 I P s e c のポリシーを一括管理する機能を前記 I P s e c 設定サーバ装置に備えている。

【0019】

本発明による他のネットワークは、上記の構成のほかに、前記要求メッセージを受信した場合に当該要求メッセージを送信した I P s e c 处理装置の通信相手の I P s e c 处理装置に対して当該通信用の要求メッセージを送信させるために要求起動メッセージを送信する機能を前記 I P s e c 設定サーバ装置に具備している。

【0020】

本発明による別のネットワークは、上記の構成のほかに、前記 I P s e c の暗号化及び認証に使用するための共有秘密鍵を生成する機能と、その生成した前記共有秘密鍵を前記 I P s e c 处理装置に配布する機能とを前記 I P s e c 設定サーバ装置に具備している。

【0021】

本発明による I P s e c 設定サーバ装置は、異なる 2 つの拠点間をインターネットを介して通信する場合にインターネット経路上でのセキュリティを確保するための I P s e c (Internet Protocol security protocol) を使用する I P s e c 处理装置の I P s e c 設定を管理する I P s e c 設定サーバ装置であって、前記 I P s e c 处理装置間に適用する前記 I P s e c のポリシーを一括管理する機能を備えている。

【0022】

本発明による他の I P s e c 設定サーバ装置は、上記の構成のほかに、前記要求メッセージを受信した場合に当該要求メッセージを送信した I P s e c 处理装置の通信相手の I P s e c 处理装置に対して当該通信用の要求メッセージを送信させるために要求起動メッセージを送信する機能を具備している。

【0023】

本発明による別の I P s e c 設定サーバ装置は、上記の構成のほかに、前記 I P s e c の暗号化や認証に使用するための共有秘密鍵を生成する機能と、その生成した前記共有秘密鍵を前記 I P s e c 处理装置に配布する機能とを具備してい

る。

【0024】

本発明によるIPsec処理装置は、インターネットにおいてIPsec (Internet Protocol security protocol) を使用するIPsec処理装置であって、前記IPsecを適用すべきパケットを受信した場合にIPsec設定サーバ装置で一括管理される当該IPsecに関する設定を前記IPsec設定サーバ装置に問い合わせるか否かを判断する機能を備えている。

【0025】

本発明による他のIPsec処理装置は、上記の構成において、前記IPsec設定サーバ装置から前記要求メッセージを送信させるための要求起動メッセージを受信した時に当該要求メッセージの送信を行っている。

【0026】

本発明による別のIPsec処理装置は、上記の構成のほかに、前記IPsecの暗号化や認証に使用するための共有秘密鍵を前記IPsec設定サーバ装置から取得する機能を具備している。

【0027】

本発明によるIPsec設定方法は、異なる2つの拠点間をインターネットを介して通信する場合にインターネット経路上でのセキュリティを確保するためのIPsec (Internet Protocol security protocol) を使用するIPsec処理装置と、前記IPsec処理装置のIPsec設定を管理するIPsec設定サーバ装置とからなるネットワークのIPsec設定方法であって、前記IPsec処理装置間に適用する前記IPsecのポリシーを一括管理するステップを前記IPsec設定サーバ装置に備えている。

【0028】

本発明による他のIPsec設定方法は、上記の動作において、前記要求メッセージを受信した場合に当該要求メッセージを送信したIPsec処理装置の通信相手のIPsec処理装置に対して当該通信用の要求メッセージを送信するために要求起動メッセージを送信するステップを前記IPsec設定サーバ装置

に具備している。

【0029】

本発明による別のIPsec設定方法は、上記のステップのほかに、前記IPsecの暗号化や認証に使用するための共有秘密鍵を生成するステップと、その生成した前記共有秘密鍵を前記IPsec処理装置に配布するステップとを前記IPsec設定サーバ装置に具備している。

【0030】

すなわち、本発明のIPsec設定方法は、インターネットにおいてIPsec (Internet Protocol security protocol) を使用するIPsec処理装置において、個々のIPsec処理装置に設定するポリシーをIPsec設定サーバに一括して登録することによって、個々のIPsec処理装置に設定するポリシーの数を削減するものである。

【0031】

また、本発明のIPsec設定方法では、上記構成において、要求メッセージを受信した場合に当該要求メッセージを送信したIPsec処理装置の通信相手のIPsec処理装置に対して当該通信用の要求メッセージを送信させるために要求起動メッセージを送信することによって、各IPsec処理装置間に適用するIPsecのポリシーの設定がそれらの装置でほぼ同時に行われることとなり、ポリシー設定後の暗号化や復号を滞りなく行うことが可能となる。これによつて、送信先のIPsec処理装置において送信元からのパケットを取りこぼしなく受取ることが可能となる。

【0032】

さらに、本発明のIPsec設定方法では、上記構成において、IPsec設定サーバが要求起動メッセージの送信時にそれに応答した要求メッセージを受信しなければ、送信元のIPsec処理装置に応答なしエラーメッセージを送信するので、送信元のIPsec処理装置で対向装置の不存在を認識することが可能となる。

【0033】

さらにもた、本発明のIPsec設定方法は、上記構成において、IPsec

の暗号化や認証に使用するための共有秘密鍵を各 I P s e c 処理装置が I P s e c 設定サーバから取得することによって、複雑な鍵交換演算を省略し、 I P s e c 処理開始までの時間を短縮するものである。

【0034】

より具体的に説明すると、本発明の I P s e c 設定方法では、 I P s e c 設定サーバが各 I P s e c 処理装置間に適用する I P s e c のポリシーを記憶している。送信元の I P s e c 処理装置が相手先の I P s e c 処理装置にデータ通信パケットを送信する場合、送信元の I P s e c 処理装置は必要な設定を I P s e c 設定サーバに要求する。要求を受信した I P s e c 設定サーバは相手先の I P s e c 処理装置に対しても設定を要求するように指示する。

【0035】

相手先の I P s e c 処理装置からの要求を受信した時点で、 I P s e c 設定サーバは登録済みのポリシーと、送信元及び相手先の両方の I P s e c 処理装置から通知された S P I (S e c u r i t y P a r a m e t e r s I n d e x : セキュリティパラメータインデックス)、及び I P s e c 設定サーバが生成した共有秘密鍵をそれぞれの I P s e c 処理装置に送信する。この時点で送信元及び相手先の両方の I P s e c 処理装置には I P s e c 処理に必要な情報がすべて揃い、 I P s e c 処理を実行することが可能となる。尚、設定情報の送受信については、従来の I P s e c によって保護することによって、第3者による盗聴を防ぐ。

【0036】

このように、本発明では、 I P s e c ポリシーを I P s e c 設定サーバで一括して管理することによって、全体の設定数を削減すると同時に、2拠点間での設定内容が異なるために発生する通信障害を防止することが可能となる。

【0037】

また、本発明では、要求起動メッセージを送信しているので、要求メッセージの送信元の I P s e c 処理装置に対向する I P s e c 処理装置ではその送信元の I P s e c 処理装置での I P s e c のポリシーの設定とほぼ同時に I P s e c のポリシーの設定が行われることとなり、そのポリシーの設定後に、送信元の I P

s e c 处理装置がパケットを暗号化して送信すると、対向する I P s e c 处理装置では送信元の I P s e c 处理装置からのパケットを復号して受取ることが可能となる。これによって、送信先の I P s e c 处理装置において送信元からのパケットを取りこぼしなく受取ることが可能となる。

【0038】

さらに、本発明では、要求起動メッセージの送信時にそれに応答した要求メッセージが対向する I P s e c 处理装置から送られてこなければ、送信元の I P s e c 处理装置に対して応答なしエラーメッセージが送信されるので、送信元の I P s e c 处理装置で対向装置の不存在を即座に認識することが可能となる。

【0039】

さらにまた、本発明では、共有秘密鍵の取得に IKE (Internet Key Exchange：自動鍵管理プロトコル) を用いないため、IKEで使用するDiffie-Hellmanの演算をする必要がない。したがって、Diffie-Hellmanの演算を必要とする従来の手法と比較して、I P s e c 处理開始までの時間を短縮することが可能となる。

【0040】

従来の手法ではIKEのSA (Security Association) を更新するためにDiffie-Hellmanの演算が定期的に発生し、そのたびに演算負荷が発生する。I P s e c による通信相手が多いほど、IKEのSAを更新する機会も増えるので、演算負荷も増加し、I P s e c 处理装置全体の処理性能が低下する。

【0041】

これに対し、本発明では、I P s e c 处理装置とI P s e c 設定サーバとの間以外の通信については、Diffie-Hellmanの演算を行わないため、従来の手法と比較して、演算負荷も軽減することが可能となる。

【0042】

【発明の実施の形態】

次に、本発明の実施例について図面を参照して説明する。図1は本発明の一実施例による I P s e c (Internet Protocol security)

y protocol) によるネットワークの構成を示すブロック図である。図1において、本発明の一実施例によるネットワークは互いにIPsec適用通信を実施しようとする複数台のIPsec処理装置2a～2fがインターネット100を介して接続され、同じくインターネット100上にIPsec設定サーバ1を接続して構成している。尚、図1に示すように、IPsec処理装置2a～2fはそれぞれの背後に存在するプライベートネットワーク201～204をIPsecによる通信によって相互に接続するルータであってもよいし、自分自身の通信にIPsecを適用するパーソナルコンピュータ（以下、パソコンとする）であってもよい。

【0043】

図2に図1のIPsec設定サーバ1の構成を示すブロック図である。図2において、IPsec設定サーバ1はインターフェース（I/F）部11と、IPsec処理部12と、SPD（Security Policy Database）13と、SAD（Security Association Database）14と、要求処理部15と、配布ポリシー記憶部16と、管理テーブル17と、乱数生成器18と、タイマ19と、記録媒体20とから構成されている。ここで、IPsec設定サーバ1は主にコンピュータから構成され、コンピュータが記録媒体20に格納されたプログラムを実行することで上記の各部の動作が実現される。

【0044】

インターフェース部11はインターネット100に接続され、インターネット100を介したデータ通信を行う。IPsec処理部12はインターフェース部11から受信したデータ通信パケットに対してIPsec処理を実施する。

【0045】

SPD13はIPsec処理部12から参照され、IPsecを適用するためのポリシーを記録している。SAD14はIPsec処理部12から参照され、個々の通信に対してIPsec処理を実施するために必要なSA（Security Association）を記録している。

【0046】

要求処理部15はインターフェース部11経由でIPsec処理装置2a～2fから設定要求メッセージを受信し、配布メッセージを返す。配布ポリシー記憶部16は要求処理部15から参照され、要求された設定を決定するために必要なIPsecポリシーが記憶されている。管理テーブル17は要求処理部15から参照、設定され、設定要求を受けた各々のSA通信に関する情報が記憶されている。

【0047】

乱数生成器18は要求処理部15からの要求によって乱数を生成する。タイマ19は要求処理部15から要求され、時間を計測する。これらの中でIPsec処理部12、SAD14、SPD13はIPsec設定サーバ1がIPsec処理装置2との通信をIPsecによって保護するために必要となるだけであり、従来のIPsecの機構と同一である。

【0048】

インターフェース部11はインターネット100からデータ通信パケットを受信すると、そのデータ通信パケットをIPsec処理部12に転送し、またIPsec処理部12から転送されたデータ通信パケットをインターネット100に送信する。

【0049】

IPsec処理部12はインターネット100から受信したIPsec適用済みのデータ通信パケットに対してSAD14やSPD13の記憶内容を基にIPsecの復号処理を行い、IPsec適用前の状態にして要求処理部15に転送する。また、IPsec処理部12は要求処理部15から受信したデータ通信パケットに対してSPD13及びSAD14の記憶内容にしたがってIPsec処理を適用し、インターフェース部11に転送する。IPsec処理部12はIPsec設定サーバ1とIPsec処理装置2a～2fとの間の通信を保護するために必要な機構であり、従来のIPsecと全く同じものである。

【0050】

図3は図2の配布ポリシー記憶部16の記憶内容を示す図である。図3において、配布ポリシー記憶部16には配布ポリシーを特定するためのアドレスペア欄

と、配布する IPsec ポリシーを設定する配布ポリシー欄とがある。配布ポリシー記憶部 16 の配布ポリシーに設定可能なパラメータは IPsec プロトコル、カプセル化モード、暗号化アルゴリズム、認証アルゴリズム、SA の有効期間である。

【0051】

図3に示す例では、IPsec 处理装置 2a – IPsec 处理装置 2b 間の通信に適用する IPsec ポリシー、IPsec 处理装置 2d – IPsec 处理装置 2e 間の通信に適用する IPsec ポリシーが設定されている。尚、配布ポリシー記憶部 16 には予めすべての項目をユーザが設定しておく必要がある。また、一度設定した後は動作中に自動的に書換えられることはない。

【0052】

IPsec 处理装置 2a – IPsec 处理装置 2b 間の配布ポリシーとしては、IPsec プロトコルに「ESP (Encapsulating Security Payload : カプセル化セキュリティペイロード)」、カプセル化モードに「トンネルモード」、暗号化アルゴリズムに「DES-CBC (Data Encryption Standard-Cipher Block Chaining)」、認証アルゴリズムに「HMAC (Hashing Message Authentication Code) –MD5-96」、SA の有効期間に「3600秒」が設定されている。

【0053】

また、IPsec 处理装置 2d – IPsec 处理装置 2e 間の配布ポリシーとしては、IPsec プロトコルに「ESP」、カプセル化モードに「トランSPORTモード」、暗号化アルゴリズムに「3DES-CBC」、認証アルゴリズムに「HMAC-SHA-1-96」、SA の有効期間に「3600秒」が設定されている。

【0054】

従来の手法では適用する IPsec ポリシーの内容についてそれぞれの IPsec 处理装置 2a ~ 2f に個別に同一の設定を入力する必要があるが、本発明の手法では IPsec 处理装置 2a ~ 2f 間の IPsec 通信に対しては配布ポリ

シー記憶部 16 のみに I P s e c ポリシーを設定すればよいため、誤ってそれぞれの I P s e c 処理装置 2 a ~ 2 f に異なる設定をしてしまう事故を回避することができると同時に、ユーザが実際に入力する設定の数も減らすことができる。

【0055】

図 4 は図 2 の管理テーブル 17 の記憶内容を示す図である。図 4 において、管理テーブル 17 には I P s e c 処理装置 2 a ~ 2 f から送られる要求メッセージに含まれる要求元アドレス、相手先アドレス、ID、S P I (S e c u r i t y Parameter Index : セキュリティパラメータインデックス) をそれぞれ記録する要求元アドレス欄、相手先アドレス欄、要求 ID 欄、S P I 欄と、当該通信用の I P s e c 処理に必要となるパラメータ群を記録する設定パラメータ欄とがある。このうち、設定パラメータ欄には当該通信に適用するポリシー及び当該通信用 S A の構築に必要なパラメータからなる S A パラメータが設定される。

【0056】

図 5 は図 4 の S A パラメータの内容を示す図である。図 5 において、S A パラメータは I P s e c プロトコル、カプセル化モード、暗号化アルゴリズム、認証アルゴリズム、有効期限、暗号鍵、認証鍵、I V (Initializat ion Vector) と、当該通信の受信側 I P s e c 処理装置 2 a ~ 2 f で使用する S P I 値からなる。

【0057】

1 個の I P s e c 通信に対して、通信を行う両端の I P s e c 処理装置 2 a ~ 2 f から要求が発生するため、管理テーブル 17 の 1 個のエントリには要求元アドレス、相手先アドレス、要求 ID、S P I は 2 個ずつ存在する。また、同一の I P s e c 通信であっても、S A の有効期限満了に備えて新しい S A が要求される場合があり、この場合には管理テーブル 17 には新しい S A のために新しく 1 個のエントリが登録される。尚、管理テーブル 17 の内容はすべて要求処理部 15 によって自動的に設定されるため、管理テーブル 17 の内容をユーザが直接設定する必要はない。

【0058】

管理テーブル 17 を参照することで、 I P s e c 処理装置 2 a ~ 2 f に配布する設定パラメータを得ることができる。設定パラメータ内の S A パラメータは I P s e c 通信を実施するそれぞれの I P s e c 処理装置 2 a ~ 2 f からの要求メッセージを受信することで確定するため、片方の I P s e c 処理装置 2 a ~ 2 f からしか要求メッセージを受信していない場合には、相手側の要求 I D 欄及び S P I 欄が空欄となり、設定パラメータ欄の S A パラメータも空欄となる。但し、適用ポリシーについては片方の I P s e c 処理装置 2 a ~ 2 f から要求メッセージを受信するだけで確定するため、片方の I P s e c 処理装置 2 a ~ 2 f から要求メッセージを受信するだけで、適用するポリシーが設定される。

【0059】

図 4 に示す例では、1 番目のエントリに I P s e c 処理装置 2 a と I P s e c 処理装置 2 b との通信に適用されるポリシー及び S A パラメータがそれぞれ登録されている。2 番目のエントリには同じく I P s e c 処理装置 2 a と I P s e c 処理装置 2 b との通信に適用されるポリシーが登録されているが、 I P s e c 処理装置 2 b から対応する設定要求メッセージを受信していないため S A パラメータが確定していない。

【0060】

図 5 に図 4 内の S A パラメータ (a) の内容を示す。 S A パラメータは配布ポリシーの内容、設定要求メッセージで通知された S P I 、及び乱数生成器 18 から得られる乱数を基に要求処理部 15 によって生成される。

【0061】

要求処理部 15 は I P s e c 処理装置 2 a ~ 2 f から要求メッセージを受信して、 I P s e c 処理装置 2 a ~ 2 f に要求起動メッセージや配布メッセージ、エラーメッセージを送信する。

【0062】

図 6 は本発明の一実施例による要求メッセージの一例を示す図である。図 6 において、要求メッセージには要求メッセージを他の要求メッセージと区別するための I D 「1001」と、要求メッセージを送信した I P s e c 処理装置 2 a ~ 2 f のアドレスを示す要求元アドレス「 I P s e c 処理装置 2 a 」と、相手とな

るIPsec処理装置2a～2fのアドレスを示す相手先アドレス「IPsec処理装置2b」と、要求元で使用するSPIの値「5100」とが含まれている。

【0063】

尚、本実施例では2台のIPsec処理装置2a～2f間に存在するIPsec通信を1種類に限定しているため、両方のIPsec処理装置2a～2fのアドレスが決まれば、適用するIPsecポリシーを一意に特定することができる。したがって、要求メッセージにはIPsec通信の両端のアドレスを設定している。これ以外に、2台のIPsec処理装置2a～2f間に複数のIPsec通信を設定したい場合が考えられる。そのような場合には、それぞれのIPsec通信を特定するために必要な情報（例えば、プロトコル番号やポート番号等）を要求メッセージに設定する。

【0064】

図7は本発明の一実施例による配布メッセージの一例を示す図であり、図8は本発明の一実施例による要求起動メッセージの一例を示す図であり、図9は本発明の一実施例による該当なしエラーメッセージの一例を示す図であり、図10は本発明の一実施例による内容不一致エラーメッセージの一例を示す図であり、図11は本発明の一実施例による応答なしエラーメッセージの一例を示す図である。

【0065】

図12及び図13は本発明の一実施例によるIPsec設定サーバ1の動作を示すフローチャートである。これら図1～図13を参照して本発明の一実施例によるIPsec設定サーバ1の動作について説明する。まず、要求処理部15が要求メッセージを受信した場合の動作について説明する。

【0066】

要求処理部15はIPsec処理装置2a～2fから要求メッセージを受信すると（図12ステップS1）、管理テーブル17の中から要求メッセージに含まれる要求元アドレス、相手先アドレス、IDが一致するエントリを検索する（図12ステップS2）。

【0067】

要求処理部15は一致するエントリが見つかると、一致したエントリのS P Iが要求メッセージに含まれるS P Iと一致するかどうかを確認する（図12ステップS3）。要求処理部15はS P Iが一致しなければ、I P s e c処理装置2a～2fに内容不一致エラーメッセージを送信する（図12ステップS8）。

【0068】

この時、内容不一致エラーメッセージには要求メッセージに含まれるI D、要求元アドレス、相手先アドレスと、エントリー一覧とを設定する。エントリー一覧には管理テーブル17に含まれるエントリの中で、要求元アドレスと相手先アドレスとが一致するすべてのエントリを設定する。但し、エントリー一覧に設定する項目は各エントリの要求I Dとそのエントリで使用される要求元アドレス用のS P Iだけである。

【0069】

I P s e c処理装置2a～2fは内容不一致エラーメッセージを受信することでI P s e c設定サーバ1が管理している設定情報と、I P s e c処理装置2a～2fが把握している設定情報との差分を知ることができる。

【0070】

この内容不一致エラーメッセージの一例を図10に示す。図10において、I P s e c設定サーバ1上においてI P s e c処理装置2aとI P s e c処理装置2bとの通信用にすでに「1001」、「1002」という要求I Dによって設定情報が生成されており、そこで使用しているS P Iの値がそれぞれ「5100」、「5110」であることがわかる。

【0071】

要求処理部15は管理テーブル17の中に要求メッセージに含まれる要求元アドレス、相手先アドレス、I Dと一致するエントリが見つかってS P Iの内容も一致した場合、管理テーブル17内の当該エントリの相手側の要求I D欄を確認する（図12ステップS4）。

【0072】

要求処理部15は相手側の要求I D欄が設定されている場合、すでに管理テー

ブル 17 の設定パラメータ欄が確定しているため、要求メッセージの送信元に配布メッセージを送信する（図 12 ステップ S5）。配布メッセージには要求メッセージに含まれる要求元アドレス、送信元アドレス、ID を設定し、設定パラメータには管理テーブル 17 内の配布ポリシーと SA パラメータとを設定する。この場合は、すでに返送すべき設定パラメータがすべて確定している場合である。

【0073】

この配布メッセージの一例を図 7 に示す。図 7 に示す例では、設定パラメータには配布ポリシー (a) と SA パラメータ (a), SA パラメータ (b) が設定されている。IPsec 处理装置 2a は配布ポリシー (a) と SA パラメータ (a), SA パラメータ (b) とを使用して双方の IPsec 通信を実施することができる。

【0074】

要求処理部 15 は管理テーブル 17 の中に要求メッセージに含まれる要求元アドレス、相手先アドレス、ID と一致するエントリが見つかって SPI の内容も一致した場合で、相手側の要求 ID 欄が設定されていなかった場合、そのまま処理を終了する（図 12 ステップ S6）。この場合には、すでに IPsec 处理装置 2a～2f から同一の要求メッセージを受信しているが、相手側の情報がないため、相手側の情報を待っている状態である。

【0075】

要求処理部 15 は管理テーブル 17 の中に要求元アドレス、相手先アドレス、ID が一致するエントリがなかった場合、要求メッセージに含まれる要求元アドレス、相手先アドレス、SPI をキーにして管理テーブル 17 を検索する（図 12 ステップ S7）。

【0076】

要求処理部 15 は一致するエントリが見つかると、要求メッセージの送信元に内容不一致エラーメッセージを送信して処理を終了する（図 12 ステップ S8）。これは既に IPsec 設定サーバ 1 に登録済みの SPI を重複して使用して IPsec 处理装置 2a～2f が新しい設定パラメータを要求した場合である。IPsec 处理装置 2a～2f は内容不一致エラーメッセージを受信することで、

S P I の重複を検出し、重複しない S P I を選択することができる。

【0077】

要求処理部15は管理テーブル17の中に要求元アドレス、相手先アドレス、IDが一致するエントリがなく、S P I の重複も検出されなければ、要求メッセージに含まれる要求元アドレスと相手先アドレスとをキーにして管理テーブル17を検索する（図12ステップS9）。この時、要求処理部15は要求ID欄が空欄のエントリを検索する。

【0078】

一致するエントリが存在した場合には、すでに相手側のIPsec処理装置2a～2fから当該通信に対する要求メッセージが送信されており、設定パラメータの適用ポリシーまで確定している状態である。要求処理部15は空欄になっている要求ID欄及びS P I 欄に要求メッセージに設定されているID及びS P I を設定し、設定パラメータ欄の適用ポリシーで示されるポリシーにしたがって、それぞれの方向用にSAパラメータを生成する。

【0079】

具体的に述べると、IPsecプロトコル、カプセル化モード、暗号化アルゴリズム、認証アルゴリズム、有効期限については適用ポリシーと同一の内容を設定し、暗号化鍵、認証鍵、IVについては乱数生成器18から乱数を取得して値を決定し、受信側S P I 欄には受信側のIPsec処理装置2a～2fが使用するS P I の値を設定する。

【0080】

要求処理部15はそれぞれの方向用のSAパラメータが生成できたら、管理テーブル17の設定パラメータ欄に登録する（図12ステップS10）。要求処理部15は管理テーブル17にSAパラメータを登録すると、要求メッセージの送信元であるIPsec処理装置2a～2fの要求IDと、設定パラメータを設定した配布メッセージをIPsec処理装置2a～2fに送信すると同時に、相手先となるIPsec処理装置2a～2fに対しても、相手先の要求IDを含む配布メッセージを送信する（図12ステップS11）。

【0081】

また、要求処理部15はタイマ19を使用してSAパラメータの有効期限と同じ時間を計測し、タイマ19が満了した時点で、管理テーブル17の当該エントリを削除する。

【0082】

要求処理部15は管理テーブル17の中に要求元アドレスと要求IDとが一致するエントリがなく、要求元アドレスと相手先アドレスとをキーとした検索でも一致するエントリがなかった場合、要求メッセージに含まれる要求元アドレスと相手先アドレスとの組をキーにして配布ポリシー記憶部16を検索する（図13ステップS21）。

【0083】

要求処理部15は該当するエントリが見つからなければ、IPsec処理装置2a～2fに該当なしエラーメッセージを送信する（図13ステップS26）。該当なしエラーメッセージには要求メッセージに含まれていたID、要求元アドレス、相手先アドレスを設定する。この該当なしエラーメッセージの一例を図9に示す。

【0084】

要求処理部15は配布ポリシー記憶部16内に一致するエントリが存在した場合、管理テーブル17の新しいエントリの要求元アドレス、相手先アドレス、要求ID、SPI欄にそれぞれ要求メッセージに含まれる要求元アドレス、相手先アドレス、ID、SPIを設定する。同一エントリのもう一つの要求元アドレスには要求メッセージの相手先アドレスを、相手先アドレスには要求メッセージの要求元アドレスを設定し、要求ID、SPIは空欄とする。

【0085】

また、要求処理部15は配布ポリシー記憶部16の該当エントリに含まれる配布ポリシーを管理テーブル17の設定パラメータ欄に設定する（図13ステップS22）。この時点で、SAパラメータを生成するために必要なパラメータ群のうち、暗号化鍵、認証鍵等の共有秘密鍵、相手先IPsec処理装置2a～2fで使用するSPI以外のパラメータがすべて確定する。共有秘密鍵は乱数生成器19から得られる乱数を使用するため、相手先のSPIさえ確定すれば、SAパ

ラメータを生成することが可能となる。

【0086】

要求処理部15は配布ポリシー記憶部16内に一致するエントリが存在し、管理テーブル17に要求元のIPsec処理装置2a～2fからの要求に応じてエントリを登録した後、相手先のIPsec処理装置2a～2fに対して要求起動メッセージを送信する（図13ステップS23）。要求起動メッセージには要求メッセージの要求元アドレスを設定する。この要求起動メッセージの一例を図8に示す。

【0087】

要求処理部15は要求起動メッセージを送信すると、5秒間隔で要求起動メッセージの送信を繰り返し、要求起動メッセージの送信先のIPsec処理装置2a～2fから管理テーブル17の該当エントリに対応する要求メッセージを受信するか、要求起動メッセージを6回送信すると、要求起動メッセージの送信を停止する。繰り返し送信することによって、1個の要求起動メッセージが紛失した場合にも他の要求起動メッセージによって処理を継続することができる。

【0088】

要求処理部15は6回の要求起動メッセージ送信によって送信を停止した場合（図13ステップS24）、管理テーブル17から該当エントリを削除し（図13ステップS27）、要求メッセージの送信元のIPsec処理装置2a～2fには応答なしエラーメッセージを送信する（図13ステップS28）。応答なしエラーメッセージには、IPsec処理装置2a～2fからの要求メッセージに含まれていたID、要求元アドレス、相手先アドレスを設定する。この応答なしエラーメッセージの一例を図11に示す。

【0089】

要求処理部15は要求起動メッセージに対して、管理テーブル17の該当エントリに対応する要求メッセージを受信した場合（図13ステップS24）、要求起動メッセージの送信を停止し、要求メッセージ受信時の動作を行う（図13ステップS25）。

【0090】

タイマ19は要求処理部15に依頼されて時間を計測し、指定された時間が経過したら要求処理部15に通知する。タイマ19は同時に複数の時間を計測することができる。

【0091】

上記のように、要求起動メッセージを送信しているので、要求メッセージの送信元のIPsec処理装置に対向するIPsec処理装置ではその送信元のIPsec処理装置でのIPsecのポリシーの設定とほぼ同時にIPsecのポリシーの設定が行われることとなり、そのポリシーの設定後に、送信元のIPsec処理装置がパケットを暗号化して送信すると、対向するIPsec処理装置では送信元のIPsec処理装置からのパケットを復号して受取ることができる。よって、ポリシー設定後の暗号化や復号を滞りなく行うことができる。

【0092】

この場合、パケットの復号ができなくてそのパケットを破棄したり、パケットの復号を誤って行ったりすることないので、送信先のIPsec処理装置において送信元からのパケットを取りこぼしなく受取ることができる。

【0093】

また、要求起動メッセージの送信時にそれに応答した要求メッセージを対向するIPsec処理装置から受信しなければ、送信元のIPsec処理装置に対して応答なしエラーメッセージを送信するので、送信元のIPsec処理装置では対向装置の不存在を即座に認識することができる。

【0094】

図14は図1のIPsec処理装置2a～2fの構成を示すブロック図である。図14においてはIPsec処理装置2a～2fをまとめてIPsec処理装置2としており、IPsec処理装置2a～2fはIPsec処理装置2と同様の構成である。

【0095】

IPsec処理装置2は主にコンピュータから構成され、IPsec設定サーバ1を利用する。つまり、IPsec処理装置2はインターフェース部(I/F)21, 22と、IPsec処理部23と、SPD24と、SAD25と、設定管

理部26と、ルーティング部27と、記録媒体28とを具備し、上記の各部の動作はコンピュータが記録媒体28のプログラムを実行することで実現される。

【0096】

インターフェース部21はプライベートネットワーク200（図1のプライベートネットワーク201～204）に接続され、プライベートネットワーク200とのデータ通信を行う。インターフェース部22はインターネット100に接続され、インターネット100を介したデータ通信を行う。

【0097】

IPsec処理部23はインターフェース部21, 22から受信したデータ通信パケットに対してIPsec処理を実施する。設定管理部26はIPsec処理部23に依頼され、必要な設定をIPsec設定サーバ1に要求する。

【0098】

SPD24はIPsec処理部23及び設定管理部26から参照され、IPsecを適用するためのポリシーを記録している。SAD25はIPsec処理部23と設定管理部26とから参照され、個々の通信に対してIPsec処理を実施するために必要なSAを記録している。ルーティング部27はIPsec処理部23と設定管理部26との間でデータ通信パケットの送受信を行い、各々のデータ通信パケットの転送先を決定する。

【0099】

IPsec処理装置2の構成は図31に示す従来のIPsec処理装置の構成と比較すると、IPsec処理装置2では設定管理部26が追加されている点が異なる。また、後述するように、SPD24に新しい項目がされた点と、IPsec処理部23に新しい動作が加えられた点とが異なる。

【0100】

インターフェース部21はプライベートネットワーク200からデータ通信パケットを受信してIPsec処理部23に転送し、またIPsec処理部23から転送されたデータ通信パケットをプライベートネットワーク200に送信する。

【0101】

インターフェース部22はインターネット100からデータ通信パケットを受信し

てIPsec処理部23に転送し、またIPsec処理部23から転送されたデータ通信パケットをインターネット100に送信する。

【0102】

SPD24には個々のSPDエントリを識別し、優先順位を明確にするためのID欄と、トラヒックを選択するためのセレクタ欄、選択されたトラヒックに対する処理欄、IPsec処理を適用する場合のIPsecのパラメータ情報等を記録するIPsec適用ポリシー欄、及びSPD検索時にIPsec設定サーバ1に設定を要求するか否かを判断するための設定要求用相手アドレス欄が存在する。

【0103】

図15は図14のSPD24の内容を示す図である。図15において、SPD24は設定要求用相手アドレス欄が追加されている以外は通常のIPsecで用いられるSPDと同一のものである。尚、SPD24は送信用と受信用とが存在する。

【0104】

SPD24はIPsec処理部23がデータ通信パケットを受信した場合に、そのパケットの扱いを決定するために用いられる。IPsec処理部23はIPsecが適用されていないデータ通信パケットを受信すると、SPD24のセレクタ欄と比較して一致するエントリを探す。一致するエントリが発見されると、処理欄にしたがって当該パケットの扱いを決定する。

【0105】

処理欄には“IPsec適用”，“通過”，“廃棄”的いずれかが格納される。特に、“IPsec適用”的処理となった場合には、IPsecポリシー欄の内容にしたがって引き続きIPsecの処理が行われる。

【0106】

本実施例ではSPD24に存在する設定要求用相手アドレス欄において、処理欄が“IPsec適用”となった場合にそのIPsec適用ポリシー欄をIPsec設定サーバ1に要求するか否かを判断するために使用すると同時に、IPsec設定サーバ1に設定を要求する場合に、要求する設定パラメータを特定する

ための識別子としても使用する。

【0107】

尚、SPD24の内容は標準のIPsecと同様に、基本的に予めすべて設定しておく必要があるが、設定要求用相手アドレスを設定したエントリについてはIPsec適用ポリシーを省略することが可能である。この場合には設定管理部26がIPsec設定サーバ1から必要なIPsec適用ポリシー情報を入手し、自動的にSPD24のIPsec適用ポリシー欄を設定する。この時、IPsec設定サーバ1との通信を暗号化するための設定だけは適用ポリシーを省略することはできない。

【0108】

図15に示す例では、IPsec処理装置2a自身からIPsec設定サーバ1宛のパケットに対して適用ポリシー(z)にしたがってIPsec処理を実施し、プライベートネットワーク202宛のパケット、及びプライベートネットワーク203宛のパケットに対してIPsec処理を適用するが、そのポリシーはIPsec設定サーバ1から取得し、それ以外のすべてのパケットはIPsec処理を適用せずに通過させる設定となっている。

【0109】

図16は図15に示すSPD24の適用ポリシー(z)の一例を示す図である。図16において、IPsec適用ポリシーにはIPsec通信で使用するプロトコルやカプセル化モード、暗号化アルゴリズム、認証アルゴリズム等、適用するIPsec処理を特定するために必要な情報が設定される。

【0110】

図16に示す例では、暗号化アルゴリズムに「AES-CBC」、認証アルゴリズムに「HMAC-SHA-1-96」を使用してESPの「トランSPORTモード」を適用することと、SAの有効期間が「3600秒」であることが示されている。尚、使用するプロトコルや暗号化アルゴリズム等によって必要となるパラメータが異なるため、それぞれの適用ポリシーにおいては図16に示すパラメータ以外のパラメータが現れる場合や、図16の中の一部のパラメータが存在しない場合もある。

【0111】

従来のIPsecでは適用ポリシーをIPsec処理装置に予めすべてユーザが設定しておく必要があるが、前項で述べた通り、本実施例のSPD24では適用ポリシーの設定を省略することが可能である。その場合には設定管理部26によってIPsec設定サーバ1から取得したIPsec適用ポリシーが自動的に設定される。

【0112】

尚、IKEを使用する場合にはIKE自身に必要となるパラメータがSPD24のIPsec適用ポリシーとは独立して存在する。しかしながら、本実施例の観点から見ると、IPsec通信を行うために、本来ユーザが設定しなければならないパラメータであって、本実施例のIPsec設定サーバ1を使用することによって省略可能なパラメータである、という点においてIPsec適用ポリシーと同等である。そこで、説明を容易にするため、SPD24のIPsec適用ポリシーがIKEを使用するポリシーの場合には、そのポリシーの中にIKE用のパラメータもすべて含まれているものとして扱う。そのため、図16に示す例ではIKE用の設定パラメータも含まれている。実際の構成においては依然としてIKE自身の設定はIPsec適用ポリシーとは独立である。

【0113】

図17は図14のSAD25の内容を示す図である。図17において、SAD25には個々のIPsec通信に必要となるSAが登録される。すなわち、SAD25はSAを管理するためのデータベースである。

【0114】

SPD24のIPsec適用ポリシーでは、適用するIPsec処理（どのような種類のIPsec処理を施すか）を示すための情報が示されるが、実際にIPsec処理を行うためには追加の情報が必要となる。

【0115】

例えば、IKEを使用する場合には、IPsec処理で使用する暗号化鍵や認証鍵を相手IPsec処理装置と交換し、それらの値を使用することで初めて一つのIPsec処理が実施することができる。このように、一つのIPsec処

理を実施するために必要なパラメータ群を SA と呼ぶ。

【0116】

SAD25には個々のSADエントリを識別するためのIDと、IPsec通信の相手アドレスを示す終点アドレスと、IPsec通信で使用されるIPsecプロトコルと、個々のSAに固有の識別子であるSPI及びその他のSAパラメータとによって構成される。

【0117】

SAD25は設定管理部26あるいはIPsec処理部23によって自動的に設定されるため、SAD25をユーザが直接設定する必要はない。尚、SAD25は標準のIPsecで用いられるSADと同一のものであり、送信用と受信用とが存在する。

【0118】

図17に示す例では、1番目のエントリにIPsec処理装置2aとIPsec処理装置2bとの間のSAが、2番目のエントリにIPsec処理装置2aとIPsec設定サーバ1との間のSAが登録されている。

【0119】

図18は図14のIPsec処理部23の処理動作を示すフローチャートであり、図19及び図20は図14の設定管理部26の処理動作を示すフローチャートである。これら図18～図20を参照してIPsec処理装置2a～2fの動作について説明する。

【0120】

IPsec処理部23はプライベートネットワーク200からインターネット100宛のデータ通信パケットを受信すると（図18ステップS31）、データ通信パケットとSPD24のセレクタ欄とを比較して該当するエントリを検索する（図18ステップS32）。該当するエントリの設定要求用相手アドレス欄が空欄の場合には、従来のIPsecと同一の動作である（図18ステップS33）。

【0121】

尚、この従来のIPsecの動作によって、IPsec処理装置2とIPse

c 設定サーバ1とのメッセージの送受信は保護される。すなわち、予め通常の I Psec の方法に従って I Psec 処理装置 2 と I Psec 設定サーバ1との間の通信については SPD24 に登録しておく。

【0122】

I Psec 処理部 23 は SPD24 の検索で該当するエントリの設定要求用相手アドレス欄が設定されていた場合で、 I Psec 適用ポリシー欄が設定されている場合、さらに SAD25 から当該通信用の SA を検索する（図 18 ステップ S34）。当該通信用の SA が存在する場合には、従来の I Psec と同一の動作となり、 SA の内容にしたがってデータ通信パケットに I Psec 処理を適用する（図 18 ステップ S33）。

【0123】

I Psec 処理部 23 は SPD24 の検索で該当するエントリの設定要求用相手アドレス欄が設定されており、 I Psec 適用ポリシー欄も設定されている場合で、 SAD25 に該当エントリがない場合、あるいはそもそも I Psec 適用ポリシー欄が設定されていない場合、当該データ通信パケットの処理を一時中断し、設定管理部 26 に設定サーバから設定を取得するように依頼する（図 18 ステップ S35）。この時、設定管理部 26 には SPD24 の当該エントリの ID を通知する。

【0124】

I Psec 処理部 23 は設定管理部 26 に依頼した後、設定管理部 26 から結果が通知されるまで同一の SPD エントリに対する依頼は行わない。 I Psec 処理部 23 は設定管理部 26 から設定完了の通知を受けると（図 18 ステップ S36）、データ通信パケットの I Psec 処理を再開する（図 18 ステップ S33）。この時点では、必要なポリシー及び SA が設定管理部 26 によって設定されており、従来通りの I Psec 処理を実施するのみとなる。

【0125】

I Psec 処理部 23 は設定管理部 26 から設定失敗の通知を受けると（図 18 ステップ S33）、一時中断していたデータ通信パケット処理を中止する（図 18 ステップ S37）。

【0126】

IPsec処理部23はインターネット100からプライベートネットワーク200宛のIPsec適用済みデータ通信パケットを受信した場合、従来のIPsecと同様に動作する。すなわち、IPsec処理部23はSAD24から該当するエントリを検索し、一致するエントリが存在した場合、その内容にしたがってIPsecの復号処理を実施する。IPsec処理部23は一致するエントリが存在しない場合、そのデータ通信パケットを廃棄する。

【0127】

IPsec処理部23は従来のIPsecと同様に、SAD25内の各SAエントリの有効期限を確認し、有効期限が満了する前に新しいSAの確立を行う。この時、当該SAがIPsec設定サーバ1によって生成されたSAだった場合、IPsec処理部23は設定管理部26にIPsec設定サーバ1から設定を取得するように依頼する。

【0128】

設定の取得を依頼する時、IPsec処理部23は設定管理部26に当該SAに対応するSPD24エントリのIDを通知する。設定管理部26からは依頼に対する結果が通知されるが、IPsec処理部23はその結果の通知を無視する。

【0129】

設定管理部26はIPsec処理部23から設定取得の依頼を受けると（図19ステップS41）、通知されたSPD24のエントリ用の要求メッセージを生成する（図19ステップS42）。要求メッセージにはIDと、要求元アドレスと、相手先アドレスと、要求元で使用するSPIの値とを設定する。IDには他の要求メッセージと重複しない任意の数値を設定し、SPIにはIPsec通信において自己が使用するつもりのSPIを設定する。要求元アドレスにはIPsec処理装置2のアドレスを設定する。相手先アドレスには、当該SPD24のエントリに含まれる設定要求用相手アドレスを設定する。

【0130】

IPsec設定サーバ1からの応答メッセージには設定管理部26が送信した

メッセージのIDと要求元アドレス、相手先アドレスが含まれるため、設定管理部26はどのメッセージに対する応答なのかを識別することができる。

【0131】

この要求メッセージの一例を図6に示す。図6に示す例はIPsec処理装置2aがIPsec処理装置2bとのIPsec通信に必要な設定を要求する要求メッセージの例である。

【0132】

設定管理部26は生成した要求メッセージをIPsec設定サーバ1に送信する（図19ステップS43）。設定管理部26はIPsec設定サーバ1に要求メッセージを送信すると、5秒間隔で要求メッセージの送信を繰り返し、IPsec設定サーバ1から要求メッセージに対応する応答を受信するか、要求メッセージを6回送信すると、要求メッセージの送信を停止する。

【0133】

設定管理部26は6回の要求メッセージ送信によって送信を停止した場合や、該当なしエラーメッセージあるいは応答なしエラーメッセージを受信した場合（図19ステップS44, S47）、IPsec処理部23に設定失敗を通知して処理を終了する（図19ステップS49）。

【0134】

尚、設定管理部26は要求メッセージの送信を繰り返す場合、常に同じID、同じSPIを使用して送信する。繰り返し送信することによって、1個の要求メッセージが紛失した場合にも他の要求メッセージによって処理を継続することができる。

【0135】

設定管理部26はIPsec設定サーバ1から内容不一致エラーメッセージを受信した場合（図19ステップS47）、内容不一致エラーメッセージに含まれるエントリー一覧を確認し、エントリー一覧に含まれるID及びSPI以外の値を用いて改めてIDとSPIとを選択し、要求メッセージをIPsec設定サーバ1に送信する（図19ステップS48）。

【0136】

これは I P s e c 標準装置 2 が何らかの原因で動作情報を喪失した後、既に I P s e c 設定サーバ 1 側に登録済みの ID あるいは SPI を使用して要求メッセージを送信した場合である。

【0137】

設定管理部 2 6 は内容不一致エラーメッセージで通知された ID や SPI 以外の値を使用することで、 I P s e c 設定サーバ 1 の既存の情報と矛盾しない新しい要求メッセージを生成することができる。

【0138】

設定管理部 2 6 は I P s e c 設定サーバ 1 から配布メッセージを受信した場合（図 19 ステップ S 4 4）、配布メッセージに含まれる適用ポリシーを当該 SPD 2 4 の I P s e c 適用ポリシー欄に設定し、配布メッセージに含まれる SA パラメータを使用して SA を生成し、 SAD 2 5 に登録する（図 19 ステップ S 4 5）。設定管理部 2 6 は SA を SAD 2 5 に登録したら、 I P s e c 標準装置 2 3 に設定完了を通知し、処理を終了する（図 19 ステップ S 4 6）。

【0139】

設定管理部 2 6 は I P s e c 設定サーバ 1 から要求起動メッセージを受信した場合（図 20 ステップ S 5 1）、SPD 2 4 のエントリの中から、設定要求用相手アドレスが要求起動メッセージに含まれる相手先アドレスと一致するエントリを検索する（図 20 ステップ S 5 2）。一致するエントリが見つからない場合、設定管理部 2 6 は要求起動メッセージを無視する（図 20 ステップ S 5 3）。

【0140】

この場合、 I P s e c 設定サーバ 1 からは 6 回要求起動メッセージが送信されるが、その後、 I P s e c 設定サーバ 1 は要求起動メッセージの送信を停止し、元々要求メッセージを送信した I P s e c 標準装置 2 には I P s e c 設定サーバ 1 からエラーメッセージが送信される。

【0141】

設定管理部 2 6 は SPD 2 4 の検索によって一致するエントリを見つけた場合、 I P s e c 標準装置 2 3 から SPD 2 4 のエントリに対する設定取得依頼を受信した時と同様に動作する。すなわち、設定管理部 2 6 は要求メッセージを生成し

て I P s e c 設定サーバ 1 に最大 6 回繰り返し送信する（図 2 0 ステップ S 5 4 , S 5 5）。

【0142】

但し、 I P s e c 処理部 2 3 の依頼による送信ではないので、 I P s e c 設定サーバ 1 から配布メッセージやエラーメッセージを受信しても、 I P s e c 処理部 2 3 にはその結果を通知しない（図 2 0 ステップ S 5 6 , S 5 8 , S 6 0）。

【0143】

また、設定管理部 2 3 は要求起動メッセージに対して要求メッセージの送信を開始した場合、繰り返し送信が停止するまで、同一の S P D 2 4 のエントリに対する要求起動メッセージを受信しても新たな要求メッセージの送信を行わない。

【0144】

一方、設定管理部 2 6 は I P s e c 設定サーバ 1 から配布メッセージを受信した場合（図 2 0 ステップ S 5 6）、配布メッセージに含まれる適用ポリシーを当該 S P D 2 4 の I P s e c 適用ポリシー欄に設定し、配布メッセージに含まれる S A パラメータを使用して S A を生成し、 S A D 2 5 に登録する（図 2 0 ステップ S 5 7）。

【0145】

ルーティング部 2 7 は I P s e c 処理部 2 3 から I P s e c 復号処理済みのデータ通信パケットを受信して、当該パケットが設定管理部 2 6 宛のパケットだった場合、当該パケットを設定管理部 2 6 に転送する。当該パケットが設定管理部 2 6 宛のパケットではない場合、ルーティング部 2 7 は当該パケットを送信すべきインターフェースを決定し、再び I P s e c 処理部 2 3 を介して送信すべきインターフェースに転送する。

【0146】

また、ルーティング部 2 7 は設定管理部 2 6 からのデータ通信パケットを受信し、当該パケットを送信すべきインターフェースを決定して、 I P s e c 処理部 2 3 を介して転送する。

【0147】

図 2 1 は図 2 の S P D 1 3 の内容の一例を示す図であり、図 2 2 は図 2 1 に示

すSPD13の適用ポリシー（v）の内容を示す図であり、図23は従来のIPsec処理装置のSPDの内容を示す図であり、図24は図23のSPDの適用ポリシー（j）の内容を示す図である。

【0148】

また、図25は図2の管理テーブル17のIPsec処理装置2aから要求メッセージを受信した後の内容を示す図であり、図26は図14のSPD24の設定メッセージを受信して適用ポリシーを設定した後の内容を示す図であり、図27は図2の管理テーブル17のSAを更新するために新しいエントリが生成される場合の内容を示す図であり、図28は本発明の一実施例によるIPsec処理装置2の動作を示すシーケンスチャートである。

【0149】

これら図1～図28を参照して本実施例のIPsec設定サーバ1の具体的な動作について説明する。ここでは図1の中のIPsec処理装置2aに注目し、プライベートネットワーク201からプライベートネットワーク202宛のデータ通信に対してIPsec処理装置2aがIPsec処理を実施する場合について説明する。まず、IPsec設定サーバ1、IPsec処理装置2a、IPsec処理装置2bに予め必要な設定項目について説明する。

【0150】

IPsec設定サーバ1にはIPsec処理装置2a及びIPsec処理装置2bとの間にそれぞれ安全なIPsecの経路を確保するために、従来と同様の方法で、SPD13を設定する。図21に示すように、SPD13にはIPsec設定サーバ1自身からIPsec処理装置2a、IPsec処理装置2b宛の通信に対して、それぞれ適用ポリシー（v）、適用ポリシー（w）にしたがってIPsecを適用するように設定している。

【0151】

この適用ポリシー（v）の内容を図22に示す。適用ポリシー（v）にはIPsec処理装置2aとの通信を暗号化するためのポリシーが設定されている。また、IPsec処理装置2aとの間のIPsec通信においてIKEによる鍵交換を実施するために、IKEに関するパラメータも設定しておく。

【0152】

尚、本来、IKEに関する設定はIPsec適用ポリシーとは独立に存在するものであるが、説明を容易にするために、本実施例の説明においては適用ポリシーの一部として扱う。適用ポリシー(w)の内容も適用ポリシー(v)と同様の内容である。

【0153】

これらの設定によって、IPsec設定サーバ1とIPsec処理装置2aとの間に安全なIPsecの経路が設定され、設定情報及び秘密鍵の配布を安全に行うことができる。

【0154】

SPD13にはIPsec設定サーバ1と通信するすべてのIPsec処理装置2に対して1件ずつ設定を行う必要がある。例えば、図21に示す例ではIPsec処理装置2a、IPsec処理装置2b以外にもIPsec処理装置2d、IPsec処理装置2eに対するポリシーも設定されている。

【0155】

続いて、IPsec設定サーバ1にはIPsec処理装置2a、IPsec処理装置2b間に適用するIPsecのポリシーを配布ポリシー記憶部16に設定する。配布ポリシー記憶部16の一例を図3に示す。配布ポリシー記憶部16のアドレスペア欄には、IPsec処理装置2a、IPsec処理装置2bのアドレスを、配布ポリシー欄には当該通信に適用するポリシーを設定する。

【0156】

ポリシーでは使用するIPsecプロトコル、カプセル化モード、暗号化アルゴリズム、認証アルゴリズム、SAの有効期間を設定する。また、IPsec設定サーバ1が共有秘密鍵を各IPsec処理装置2a～2fに配布するため、IPsec処理装置2a～2fはIKEを使用しない。したがって、配布ポリシーにはIKEに関するパラメータを設定する必要がない。

【0157】

配布ポリシー記憶部16にはIPsec設定サーバ1が管理する他の通信に対するポリシーをすべて設定しておく。図3に示す例では、IPsec処理装置2

a、IPsec処理装置2b間の通信以外にも、IPsec処理装置2d、IPsec処理装置2e間の通信に対するポリシーが設定されている。

【0158】

各IPsec処理装置2a～2fにはSPD24を設定する。SPD24にはIPsec設定サーバ1との通信をIPsecで暗号化するために通常のIPsecの設定を行い、実際にIPsecを適用したい通信に関しては、セレクタ欄と設定要求用相手アドレス欄とを設定する。

【0159】

IPsec処理装置2aのSPD24の一例を図15に示す。ID=1のエントリが、IPsec設定サーバ1との通信を暗号化するための設定である。この設定はIPsec設定サーバ1のSPD13に設定したものに対応している。適用ポリシー(z)の内容を図16に示す。相手先アドレス以外はIPsec設定サーバ1に設定したポリシーと同じであり、IKEに関する設定も含まれる。

【0160】

ID=2のエントリがプライベートネットワーク202宛の通信を暗号化するための設定である。セレクタ欄には対象となる通信としてプライベートネットワーク202宛の通信を設定し、処理欄にはIPsecを設定する。ここで、IPsec適用ポリシー欄は省略し、設定要求用相手アドレス欄にIPsec処理装置2bのアドレスを設定する。

【0161】

SPD24にはIPsec処理装置2aがIPsecを適用したい通信をすべて設定する。図15に示す例では、IPsec処理装置2bとの通信以外にプライベートネットワーク203宛の通信に対してIPsec処理装置2cとIPsec通信を実施する設定となっている。

【0162】

IPsec処理装置2bにも上記と同様の設定を行う。すなち、SPD24にIPsec設定サーバ1用の設定を適用ポリシーとともに設定し、他のIPsec通信に対してはセレクタと設定要求用相手アドレスとを設定しておく。

【0163】

以上が予め必要な設定となる。従来のIPsec処理装置のSPDに、上記と同様の設定を設定した例を図23に示す。従来のIPsec処理装置ではIPsec設定サーバ1用の設定が不要となるが、IPsecを適用するすべての通信についてIKEに関する設定を含む適用ポリシーを設定しなければならない。図23に示す例では、プライベートネットワーク202、プライベートネットワーク203宛の通信に対してそれぞれ適用ポリシー(j)、適用ポリシー(k)を設定している。適用ポリシー(j)の内容を図24に示す。適用ポリシー(j)にはIPsecプロトコル、カプセル化モード等のIPsec適用ポリシーに加えて、IKEのポリシーも設定する。

【0164】

ここで、n台のIPsec処理装置がすべての組み合わせで、互いにIPsecの通信を実施する場合において、本実施例によるIPsec設定サーバ1を用いた場合の設定量と従来のIPsec処理装置に必要な設定量とを比較する。IPsecのポリシーに関する設定とIKEのポリシーに関する設定とをそれぞれ「1」と数えると、従来のIPsec処理装置では、1台のIPsec処理装置に(n-1)件分のIPsecポリシーとIKEポリシーとを設定する必要があるため、1台当たりの設定量は $2(n-1)$ となり、n台で $2n(n-1)$ となる。

【0165】

これに対し、本実施例によるIPsec処理装置2ではIPsec設定サーバ1との通信用にIPsecポリシーとIKEポリシーとを1件ずつ設定するのみで、1台当たりの設定量は2となり、n台で $2n$ となる。

【0166】

IPsec設定サーバ1には、それぞれのIPsec処理装置2との通信のためにIPsecポリシーとIKEポリシーとを1件ずつ設定することによって $2n$ の設定量と、個々のIPsec処理装置2同士の通信の組合せに対してIPsecポリシーを1件設定するために $n(n-1)/2$ の設定量とが必要となり、IPsec設定サーバ1全体に必要な設定量は $2n + n(n-1)/2$ となる。

【0167】

したがって、本実施例による I P s e c 設定サーバ 1 を用いた場合の設定量は $4n + n(n - 1) / 2 = n(n + 7) / 2$ となる。例えば、 $n = 10$ の場合には従来の手法の設定量 180 に対して、本発明の設定量が 85 となり、約半分の設定で済むことになる。

【0168】

n^2 の係数に注目すれば、 n が大きくなると、本実施例における設定量が従来の手法の $1/4$ に近づくことがわかり、組合せが多くなるほど効果が大きくなることがわかる。

【0169】

続いて、I P s e c 処理装置 2 a がプライベートネットワーク 202 宛のパケットを受信した後の動作について説明する。I P s e c 処理装置 2 a がプライベートネットワーク 202 宛のパケットをインターフェース部 21 から受信すると、パケットは I P s e c 処理部 23 に渡される。

【0170】

I P s e c 処理部 23 は S P D 24 のセレクタと受信したパケットを比較して該当するエントリを探す。図 15 に示す内容とプライベートネットワーク 202 宛のパケットを比較すると、ID = 2 のエントリと一致する。I P s e c 処理部 23 は該当エントリの処理欄にしたがって I P s e c の適用を試みるが、I P s e c 適用ポリシーが設定されておらず、代わりに設定要求用相手アドレスが設定されているため、I P s e c 適用処理を一時中断し、設定管理部 26 に設定の取得を依頼する。

【0171】

設定管理部 26 は I P s e c 処理部 23 から設定取得の依頼を受けると、当該 S P D エントリ用の要求メッセージを生成する。要求メッセージの例を図 6 に示す。ID と S P I とは設定管理部 26 が任意の数値を設定し、要求元アドレスには I P s e c 処理装置 2 a 自身のアドレスを、相手先アドレスには S P D エントリの設定要求用相手アドレスである I P s e c 処理装置 2 b のアドレスを設定する。

【0172】

設定管理部26は生成した要求メッセージをIPsec設定サーバ1に送信する。設定管理部26はIPsec設定サーバ1に要求メッセージを送信すると、5秒間隔で要求メッセージの送信を繰り返し、IPsec設定サーバ1から要求メッセージに対応する応答を受信するか要求メッセージを6回送信すると要求メッセージの送信を停止する。繰り返し送信することによって、1個の要求メッセージが紛失した場合にも他の要求メッセージによって処理を継続することができる。

【0173】

設定管理部26からIPsec設定サーバ1に要求メッセージが送信される時、要求メッセージは図15に示すSPD24の1番目のエントリにしたがって、IPsec処理部23によってIPsecを適用されてからIPsec設定サーバ1に送信される。そのため、IPsec設定サーバ1に送信されるメッセージはインターネット100上の第3者に盗聴されることなく、安全に送信することができる。尚、各IPsec処理装置2からIPsec設定サーバ1に送信されるメッセージはすべて同様の手順でIPsecを適用されてから送信されるため、以下の説明ではIPsec設定サーバ1に送信するメッセージに対してIPsecを適用する手順についてはその説明を省略する。

【0174】

IPsec設定サーバ1に送信された要求メッセージはIPsec設定サーバ1のインターフェース部11に到着する。インターフェース部11で受信された要求メッセージはIPsec処理部12に送られる。IPsec処理部12ではIPsecによって暗号化された要求メッセージを元の状態に復号し、復号後のパケットを要求処理部15に送る。

【0175】

尚、各IPsec処理装置2からIPsec設定サーバ1に送られるメッセージはすべて同様の手順で要求処理部15に届くため、以下の説明ではインターフェース部11でメッセージが受信されてから要求処理部15に届けられるまでの手順についてはその説明を省略する。同様に、IPsec設定サーバ1からIPsec処理装置2に送信されるメッセージにIPsecが適用される手順について

もその説明を省略する。

【0176】

要求処理部15は要求メッセージを受信すると（図12ステップS1）、管理テーブル17からアドレス及びIDが一致するエントリを検索するが、最初は管理テーブル17には何も設定されていないため、一致するエントリが見つからない（図12ステップS2, S7, S9）。

【0177】

要求処理部15は新規登録のため、要求メッセージに含まれる要求元アドレスと相手先アドレスをキーにして配布ポリシー記憶部16の中から該当するエントリを検索する（図13ステップS21）。要求メッセージに含まれる要求元／相手先アドレスはそれぞれIPsec処理装置2a及びIPsec処理装置2bなので、図3に示す配布ポリシー記憶部16の先頭のエントリが一致する。

【0178】

配布ポリシー記憶部16に一致するエントリが見つかったので、要求処理部15は管理テーブル17の新しいエントリを選び、要求元アドレス、相手先アドレス、要求ID、SPI欄にそれぞれ要求メッセージに含まれるIPsec処理装置2aのアドレス、IPsec処理装置2bのアドレス、要求IDの「1001」、SPIの「5100」を設定する。同一エントリのもう一つの要求元アドレス、相手先アドレスにはそれぞれIPsec処理装置2bのアドレス、IPsec処理装置2aのアドレスを設定する。

【0179】

さらに、配布ポリシー記憶部16の該当エントリに設定されている配布ポリシー(a)を管理テーブル17の設定パラメータ欄に設定する（図13ステップS22）。ここまで設定を終えた管理テーブル17を図25に示す。

【0180】

要求処理部15は相手先アドレスであるIPsec処理装置2bに対して要求起動メッセージを送信する（図13ステップS23）。要求起動メッセージには、相手先アドレスとして要求メッセージの送信元アドレスであるIPsec処理装置2aのアドレスを設定する。要求起動メッセージの一例を図8に示す。

【0181】

要求処理部15はIPsec処理装置2bから要求メッセージを受信するまで、5秒間隔で最大6回要求起動メッセージを送信する。繰り返し送信することによって、1個の要求起動メッセージが紛失した場合にも他の要求起動メッセージによって処理を継続することができる。

【0182】

IPsec処理装置2bに送信された要求起動メッセージはIPsec処理装置2bのインターフェース部22に到着する。IPsec処理装置2bでは、インターフェース部22で受信された要求起動メッセージがIPsec処理部23に送られる。

【0183】

IPsec処理部23ではIPsecによって暗号化された要求起動メッセージを元の状態に復号し、復号後のパケットをルーティング部27に送る。ルーティング部27ではメッセージの宛先がIPsec処理装置2b自身であることを判断して、要求起動メッセージを設定管理部26に渡す。尚、IPsec設定サーバ1から各IPsec処理装置2に送信されるメッセージはすべて同様の手順で設定管理部26に届くため、以下の説明ではインターフェース部22でメッセージが受信されてから設定管理部26に届けられるまでの手順についてはその説明を省略する。

【0184】

設定管理部26はIPsec設定サーバ1から要求起動メッセージを受信すると、SPD24のエントリの中から、設定要求用相手アドレスがIPsec処理装置2aのアドレスと一致するエントリを検索する。IPsec処理装置2bのSPD24には予めIPsec処理装置2a用のエントリを設定済みであるため、そのエントリと一致する。

【0185】

設定管理部26は当該エントリのポリシーを取得するために要求メッセージを生成する。要求メッセージでは要求元アドレス、相手先アドレスにそれぞれIPsec処理装置2b、IPsec処理装置2aのアドレスを設定し、ID及びS

P I にはそれぞれ設定管理部26が任意に選択した要求ID「2001」、S P I 「6100」を設定する。

【0186】

設定管理部26は生成した要求メッセージをI P s e c 設定サーバ1に送信する。設定管理部26はI P s e c 設定サーバ1に要求メッセージを送信すると、5秒間隔で要求メッセージの送信を繰り返し、I P s e c 設定サーバ1から要求メッセージに対応する応答を受信するか、要求メッセージを6回送信すると、要求メッセージの送信を停止する。

【0187】

I P s e c 処理装置2bから送信された要求メッセージはI P s e c 設定サーバ1のインターフェース部11に到着し、要求処理部15に転送される。要求処理部15はI P s e c 処理装置2bから要求メッセージを受信すると、要求起動メッセージの送信を停止し、要求メッセージの受信処理（図12ステップS1）を開始する。

【0188】

要求処理部15は図25に示す管理テーブル17から要求メッセージに含まれるアドレス及びIDが一致するエントリを検索するが、IDが一致するエントリは存在しない（図12ステップS2）。また、アドレス及びS P I が一致するエントリも存在しない（図12ステップS7）。

【0189】

続いて、要求処理部15は管理テーブル17においてアドレスが一致してIDが空欄のエントリを検索する（図12ステップS9）。図25に示す最初のエントリが該当するので、要求処理部15は要求メッセージに含まれる値を使用して、空欄になっているID欄及びS P I 欄に要求ID「2001」、S P I 「6100」をそれぞれ設定する。

【0190】

さらに、I P s e c 処理装置2aからI P s e c 処理装置2bへの順方向用のSAパラメータと、逆方向用のSAパラメータとを生成する（図12ステップS10）。具体的には、I P s e c プロトコル、カプセル化モード、暗号化アルゴ

リズム、認証アルゴリズム、有効期限について配布ポリシー（a）と同一の内容を設定し、暗号化鍵、認証鍵、IVについては乱数生成器18から乱数を取得して値を設定する。

【0191】

また、受信側SPI欄には受信側となるIPsec処理装置2が使用するSPIを設定する。設定後の管理テーブル17の内容を図4に示す。1番目のエントリについて、要求IDの欄に「2001」が設定され、SPIの欄に「6100」が設定され、それぞれの方向用のSAパラメータにはSAパラメータ（a）とSAパラメータ（b）とが設定されている。SAパラメータ（a）の内容を図5に示す。逆方向のSAパラメータ（b）では暗号化鍵、認証鍵、IVとして異なる乱数値が使用されることと、受信側SPIの値がIPsec処理装置2a用の「5100」となること以外は同じ内容となる。

【0192】

要求処理部15は管理テーブル17の設定パラメータ欄の内容を使用して配布メッセージを作成し、IPsec処理装置2aとIPsec処理装置2bに対してそれぞれ送信する（図12ステップS11）。

【0193】

この時、送信する配布メッセージに設定する要求元アドレス、相手先アドレス、IDは管理テーブル17の当該エントリで示される値を使用する。したがって、IPsec処理装置2a宛の配布メッセージでは要求元アドレス、相手先アドレス、IDの値はそれぞれIPsec処理装置2aのアドレス、IPsec処理装置2bのアドレス、要求ID「1001」となり、IPsec処理装置2b宛の配布メッセージではそれぞれIPsec処理装置2bのアドレス、IPsec処理装置2aのアドレス、要求ID「2001」となる。IPsec処理装置2a宛の配布メッセージの内容を図7に示す。

【0194】

要求処理部15は配布メッセージを送信後、タイマ19を使用してSAパラメータの有効期限と同じ時間を計測し、タイマ19が満了した時点で管理テーブル17の当該エントリを削除する。

【0195】

I P s e c 設定サーバ1からI P s e c 処理装置2 aに送信された配布メッセージはI P s e c 処理装置2 aのインターフェース部2 2に到着し、設定管理部2 6に転送される。

【0196】

I P s e c 処理装置2 aの設定管理部2 6はI P s e c 設定サーバ1から配布メッセージを受信すると、要求メッセージの送信を停止し、配布メッセージに含まれる適用ポリシーをS P D 2 4のI P s e c 適用ポリシー欄に設定する。ポリシーを設定した後のS P D 2 4の内容を図2 6に示す。

【0197】

さらに、設定管理部2 6は配布メッセージに含まれるS Aパラメータを使用して、双方向の通信用にそれぞれS Aを生成し、S A D 2 5に設定する。I P s e c 処理装置2 aからI P s e c 処理装置2 b方向のS Aを設定したS A D 2 5の内容を図1 7に示す。

【0198】

S A D 2 5の1番目のエントリが該当エントリである。配布メッセージで通知されたS Aパラメータ（a）はシーケンス番号が加えられてS A D 2 5に設定されている。受信用のS A D 2 5も配布メッセージによって通知されたS Aパラメータ（b）の内容にしたがって同様に設定する。この時点でI P s e c 処理装置2 aのI P s e c 処理部2 3がI P s e c 処理装置2 b宛の通信に対するI P s e c の処理を実施できるようになる。

【0199】

設定管理部2 6はS P D 2 4及びS A D 2 5の設定を終えると、I P s e c 処理部2 3に設定完了を通知する。I P s e c 処理部2 3は設定管理部2 6から設定完了通知を受信すると、一時中断していたデータ通信パケットの処理を再開する。この時点では、S P D 2 4のエントリの適用ポリシー及び対応するS A D 2 5のエントリが存在するため、I P s e c 処理部2 3は従来通りのI P s e c 処理を実施することができる。

【0200】

IPsecを適用されたパケットはIPsec処理装置2b宛に送信される。IPsec処理装置2b側もIPsec設定サーバ1から配布メッセージを受信した時点でSPD24及びSAD25にエントリを設定しているため、IPsec処理装置2aからIPsec適用済みパケットを受信した時点で従来の手順でIPsecの復号処理を実施することができる。

【0201】

IPsec処理装置2bのIPsec処理部23によって復号処理されたパケットは、インターフェース部21からプライベートネットワーク202に送出される。このようにして、プライベートネットワーク201から送出されたパケットはプライベートネットワーク202に到達する。

【0202】

この時、さらにプライベートネットワーク201からプライベートネットワーク202宛のパケットが引き続き発生した場合について説明する。IPsec処理装置2aのIPsec処理部23は図26に示すSPD24を検索し、2番目のエントリにすでにポリシーが存在することを確認し、さらに図17に示すSAD25を検索して1番目のエントリに当該SAが存在することも確認し、当該SAを使用してIPsecの処理を実施する。すなわち、IPsec設定サーバ1から設定パラメータを取得した後は、従来のIPsecと同様に動作する。

【0203】

続いて、SA更新時の動作について説明する。IPsec処理装置2aのIPsec処理部23はSAD25を監視し、有効期限が満了するエントリについてSAの更新を実施する。

【0204】

SAを更新する場合、IPsec処理部23は設定管理部26に設定取得を依頼する。この時、IPsec処理部23は当該SAに対応するSPD24のエントリを設定管理部26に通知する。

【0205】

設定管理部26はIPsec処理部23から設定取得の依頼を受けると、当該SPDエントリ用の要求メッセージを生成する。要求メッセージではID及びS

P I 以外は最初に送信した要求メッセージと同一の内容を設定する。I D 及び S P I は新しい値を設定する。ここでは設定管理部26がI D 及びS P I の値としてそれぞれ「1002」，「5110」を選択したものとする。

【0206】

設定管理部26は生成した要求メッセージをIPsec設定サーバ1に送信する。設定管理部26はIPsec設定サーバ1に要求メッセージを送信すると、5秒間隔で要求メッセージの送信を繰り返し、IPsec設定サーバ1から要求メッセージに対応する応答を受信するか、要求メッセージを6回送信すると、要求メッセージの送信を停止する。

【0207】

IPsec設定サーバ1に送信された要求メッセージはIPsec設定サーバ1のインターフェース部11に到着し、要求処理部15に届けられる。要求処理部15は要求メッセージを受信すると（図12ステップS1）、管理テーブル17からアドレス及びI Dが一致するエントリを検索するが、I D及びS P Iがともに新しい値のため、一致するエントリが見つからない（図12ステップS2，S7）。また、この時点ではI Dが空欄のエントリも存在しない（図12ステップS9）。

【0208】

これ以降は初めて要求メッセージを受信した時の動作と同じ手順となる。すなわち、要求処理部15は配布ポリシー記憶部16を検索し（図13ステップS21）、管理テーブル17に新しくエントリを登録する（図13ステップS22）。この時点での管理テーブル17の内容を図4に示す。I D及びS P I欄がそれぞれ「1002」，「5110」であるエントリが2番目に追加されていることがわかる。

【0209】

要求処理部15は相手先となるIPsec処理装置2bに要求起動メッセージを送信する（図13ステップS23）。IPsec処理装置2bでは要求起動メッセージを受信すると、やはり新しいI DとS P Iとを設定して要求メッセージを送信する。ここでは、IPsec処理装置2bが新しいI D、S P Iとしてそ

れぞれ「2002」，「6110」を選択したものとする。

【0210】

IPsec設定サーバ1の要求処理部15はIPsec処理装置2bから要求メッセージを受信すると（図12ステップS1）、アドレスは一致するが、IDが空欄のエントリを発見し（図12ステップS9）、要求メッセージで通知されたID及びSPIと、生成したSAパラメータとを管理テーブル17に設定する（図12ステップS10）。この時点での管理テーブル17の内容を図27に示す。

【0211】

図27に示す内容を図4に示す内容と比較すると、空欄だったID，SPI欄に「2002」，「6110」が設定され、SAパラメータも設定されていることがわかる。さらに、要求処理部15は管理テーブル17の内容にしたがって配布メッセージを生成し、IPsec処理装置2a及びIPsec処理装置2bに対してそれぞれ送信する（図12ステップS11）。

【0212】

各IPsec処理装置2の設定管理部26は配布メッセージを受信すると、配布メッセージで通知されたポリシーをSPD24に設定し、通知されたSAパラメータからSAを生成してSAD25を設定する。この時点で、新しいSAが利用可能となり、SAの更新が完了する。

【0213】

ここで、IPsec処理装置2がインターフェース部21からIPsecを適用する最初のパケットを受信した後、実際にIPsec処理を実施してパケットをインターフェース部22に送信するまでの処理について、従来のIPsecによる手順と本実施例による手順とを比較する。

【0214】

従来の手法では、図32に示すように、インターフェース部41からパケットを受信すると、IPsec処理部43がIKEによる公開鍵の演算を実施し、通信相手となるIPsec処理装置と公開鍵を交換する。IPsec処理部43はさらに秘密鍵の演算を実施し、得られた秘密鍵を用いてIPsecを適用し、パケ

ットをインターフェース部22に送る。

【0215】

これに対し、本実施例の手順では、図28に示すように、IPsec処理部23がインターフェース部21からパケットを受信すると、IPsec処理部23は設定管理部26に設定取得を依頼し、設定管理部26はIPsec設定サーバ1に要求メッセージを送信する。

【0216】

設定管理部26はIPsec設定サーバ1から配布メッセージを受信すると、IPsec処理部23に設定完了を通知し、IPsec処理部23はパケットにIPsecを適用してインターフェース部22に送る。

【0217】

インターフェース部21がパケットを受信してからIPsec処理を実施してパケットをインターフェース部22に送信するまでの時間を、従来の手順、本実施例の手順についてそれぞれTb, Taとする。この時、従来の手順では公開鍵及び秘密鍵の演算に時間がかかるため、Tb > Taとなり、本実施例の手順の方が早くパケットを転送できることがわかる。

【0218】

例えば、IKEのDiffie-Hellman鍵共有アルゴリズムで使用するグループを1536ビットMODP (Modular Exponentiation Group) として50MHzのRISC (Reduced Instruction Set Computer) プロセッサを使用した場合、Tbは約18秒(実測値)となるが、Taは1秒未満となる。

【0219】

厳密には、本実施例の手順の要求メッセージは従来のIPsecの手順で送信されるため、この時、IKEの鍵交換が実施される場合にはTb < Taとなるが、それ以降のIPsec通信については相手先となるIPsec処理装置2の組合せに関係なく、IPsec設定サーバ1用のIKEのSAが有効な間はTb > Taとなる。

【0220】

また、従来の手法においてIKEの公開鍵あるいは秘密鍵の演算を実施する場合には、IPsec処理装置がIKEの演算処理に集中してしまうため、IPsecを適用する必要のないパケットの転送速度が低下してしまう。IKEの鍵交換処理は通信している相手毎に定期的に発生するため、IPsec通信をする相手が多いほど処理能力が低下する割合が大きくなる。

【0221】

それに対して本実施例の手順では、IPsec処理装置2とIPsec設定サーバ1との間で定期的に鍵交換処理が発生するが、通信相手となる各IPsec処理装置2に対しては鍵交換処理を行わないため、IPsec通信をする相手が増えたとしても処理能力が低下する割合は一定である。

【0222】

例えば、IKEのDiffie-Hellman鍵共有アルゴリズムで使用するグループを1536ビットMODP、IKEのSAの有効期限を1時間として50MHzのRISCプロセッサを使用した場合、IPsec処理装置が他の10台のIPsec処理装置との間でIPsec通信を実施すると、従来の手順では1時間の間にIKEの鍵交換が10回ずつ実施されることになり、1時間当たり約180秒間性能が低下することになる。

【0223】

それに対して、本実施例の手法では、IPsec設定サーバ1との間でIKEの鍵交換が実施されるのみなので、1時間当たり約18秒間の性能低下のみとなる。

【0224】

IKEの演算処理速度に起因する問題を解決する既存の手段として、演算専用回路をIPsec処理装置に搭載し、IKEの演算処理自体を高速化する方法がある。演算専用回路を搭載したIPsec処理装置の例を図33に示す。演算専用回路51がIPsec処理部43に接続されている点が、図31に示す従来のIPsec処理装置4と異なる。

【0225】

IPsec処理部43はIKEの演算が必要になると、演算専用回路51に演

算を依頼する。演算専用回路51によって高速に演算が実施されるため、図32に示す従来手法の演算処理に要する時間が短くなり、全体の速度も向上する。この手段を用いれば、IKEの演算速度に起因する問題を解決することが可能である。但し、演算専用回路51を持たないIPsec処理装置をすでに導入してしまっている場合には、IPsec処理装置そのものを演算専用回路付きのIPsec処理装置に置き換える必要がある。

【0226】

それに対して、本実施例の方法では必要となる機能をすべてソフトウェアで実現することができるため、すでに導入済みのIPsec処理装置に対してもソフトウェアのバージョンアップで機能を追加することが可能であり、既存の設備を有効活用することができる。

【0227】

このように、本実施例では使用するサービスやアルゴリズム等の情報をIPsec設定サーバ1に一括して設定することによって、IPsec処理装置2, 2a～2fがほとんどの設定をIPsec設定サーバ1から取得することができるため、IPsec処理装置2, 2a～2fへの設定を少なくすることができる。

【0228】

また、本実施例では、IPsec処理装置2, 2a～2fにおいてIKEを使用せずに、秘密鍵を更新することによって、IKEに関する設定が不要となるので、IPsec処理装置2, 2a～2fへの設定を少なくすることができる。

【0229】

さらに、本実施例では、IPsec設定サーバ1を用いることによって、従来、IPsecを実施する両端の装置にそれぞれ同一の設定を行う必要があるが、IPsec設定サーバ1がそれぞれの装置に設定していた内容を自装置のみに設定すればよいため、IPsec処理に関する設定の総数を少なくすることができる。

【0230】

上記のほかに、本実施例では、要求起動メッセージを送信しているので、要求

メッセージの送信元の I P s e c 処理装置に対向する I P s e c 処理装置ではその送信元の I P s e c 処理装置での I P s e c のポリシーの設定とほぼ同時に I P s e c のポリシーの設定が行われることとなり、そのポリシーの設定後に、送信元の I P s e c 処理装置がパケットを暗号化して送信すると、対向する I P s e c 処理装置では送信元の I P s e c 処理装置からのパケットを復号して受取ることができる。

【0231】

これによって、本実施例では、ポリシー設定後の暗号化や復号を滞りなく行うことができ、送信先の I P s e c 処理装置において送信元からのパケットを取りこぼしなく受取ることができ、対向する I P s e c 処理装置で送信元からのパケットを復号するまでの時間を大幅に短縮することができる。

【0232】

また、本実施例では、要求起動メッセージの送信時にそれに応答した要求メッセージが対向する I P s e c 処理装置から送られてこなければ、送信元の I P s e c 処理装置に対して応答なしエラーメッセージが送信されるので、送信元の I P s e c 処理装置で対向装置の不存在を即座に認識することができる。

【0233】

上記と同様に、本実施例では、I P s e c 設定サーバ1を用いることによって、従来、I P s e c を実施する両端の装置に同一の設定をそれぞれ個別に設定する必要があるので、設定内容の不一致が発生する可能性があるが、I P s e c 設定サーバ1が両端の装置に同一の設定を配信し、設定内容の不一致が発生しなくなるため、I P s e c の設定不一致による接続障害がなくなる。

【0234】

また、本実施例では、従来、定期的に共有秘密鍵を更新するために I K E を使用した複雑な演算が必要であるが、I K E の代わりに I P s e c 設定サーバ1から共有秘密鍵を取得することで、両端の装置が共有秘密鍵の演算を行う必要がなくなるため、I K E を使用した場合と比較して通信を開始できるまでの時間が短くなる。

【0235】

これと同様に、本実施例では、従来、定期的に共有秘密鍵を更新するためにIKEを使用した複雑な演算が必要であるが、IKEの代わりにIPsec設定サーバ1から共有秘密鍵を取得することで、両端の装置が共有秘密鍵の演算を行う必要がなくなるため、IKEを使用した場合と比較してIPsec処理を実施する装置の演算負荷を軽減することができる。

【0236】

図29は本発明の他の実施例によるIPsec処理装置の構成を示すブロック図である。図29においては、IPsec処理装置3がルータではなく、パーソナルコンピュータの場合の適用例を示している。

【0237】

本発明の他の実施例によるIPsec処理装置3はインターフェース部21を省き、上位アプリケーション部31を設けた以外は図14に示す本発明の一実施例によるIPsec処理装置2と同様の構成となっており、同一構成要素には同一符号を付してある。また、同一構成要素の動作は本発明の一実施例と同様である。

【0238】

上位アプリケーション部31はデータ通信パケットを送受信する実体であり、ルーティング部27に接続されている。ルーティング部27は送受信されるパケットが上位アプリケーション部31宛なのか、設定管理部26宛なのか、あるいはインターネット100宛なのかを判断してパケットをそれぞれの宛先に転送する。

【0239】

ここで、図1におけるIPsec処理装置2dとIPsec処理装置2eとがパーソナルコンピュータであるものとし、IPsec処理装置2dからIPsec処理装置2eに対してパケットを送信する場合について考える。

【0240】

ルータの場合と同様に、IPsec設定サーバ1にはIPsec処理装置2d、IPsec処理装置2eとの間にそれぞれ安全なIPsecの経路を確保するためにSPD13を設定し、IPsec処理装置2d、IPsec処理装置2e

間に適用するIPsecのポリシーを配布ポリシー記憶部16に設定する。

【0241】

これらIPsec処理装置2d, 2eにはSPD24を設定する。IPsec設定サーバ1との通信を暗号化するために通常のIPsecの設定を行い、実際にIPsecを適用したい通信に関しては、セレクタと設定要求用相手アドレスとを設定する。

【0242】

IPsec処理装置2dからパケットが送信される場合、パケットを送受信する実体である上位アプリケーション部31からデータ通信パケットがルーティング部27に渡される。ルーティング部27ではパケットの宛先がインターネット側であることを認識して、パケットをIPsec処理部23に転送する。

【0243】

これ以降は、ルータの場合の実施例と同じである。すなわち、IPsec処理部23はSPD24のセレクタとパケットとを比較して該当するエントリを検索し、該当するエントリに示された処理がIPsecであれば、IPsecの適用を実施する。

【0244】

この時、該当するエントリにIPsec適用のポリシーが存在しない場合、IPsec処理部23はパケットの処理を一時中断し、設定管理部26に設定要求を依頼する。設定管理部26はIPsec設定サーバ1に要求メッセージを送信し、配布メッセージを受信することでSPD24とSAD25とを設定し、IPsec処理部23に設定完了を通知する。IPsec処理部23は中断していたパケットの処理を再開し、設定されたSAを使用してIPsecを適用したうえで、パケットをインターフェース部22経由でインターネット100に転送する。

【0245】

受信時もルータの場合とほぼ同様である。IPsec処理装置2d, 2eではすでに設定管理部26によってSPD24、SAD25が設定されている。インターフェース部22経由で受信したIPsec適用済みパケットはIPsec処理部23に転送される。IPsec処理部23はSAD25から該当するSAを検

探し、パケットの復号処理を行う。

【0246】

復号処理によって元の状態に戻ったパケットはルーティング部27に転送される。ルーティング部27ではパケットが上位アプリケーション部31宛であるか、設定管理部26宛であるかを判断し、上位アプリケーション部31宛であれば上位アプリケーション部31に転送する。

【0247】

このようにすることで、パケットの受信処理が完了する。したがって、本実施例ではIPsec処理装置2d, 2eがルータの場合でもパーソナルコンピュータの場合でも適用することができる。

【0248】

図30は本発明の別の実施例による配布ポリシー記憶部の記憶内容を示す図である。本発明の一実施例ではIPsec設定サーバ1の配布ポリシー記憶部10に、実際にIPsec通信を行うIPsec処理装置2間に適用するポリシーを個々の通信毎に設定する必要があるが、本発明の別の実施例ではいくつかの組合せについて共通のポリシーを利用することで、配布ポリシー記憶部16に設定するポリシーの数を減らしている。尚、本発明の別の実施例によるIPsec設定サーバの構成は図2に示す本発明の一実施例によるIPsec設定サーバ1の構成と同様になっている。

【0249】

本実施例において、配布ポリシー記憶部16は特定のアドレスの組合せに対してポリシーを設定すると同時に、任意の組合せにおけるポリシーを設定することが可能となっている。図30に示す例では、IPsec処理装置2d、IPsec処理装置2e間の通信に適用するポリシーと、それ以外のすべての組合せに適用するポリシーとが設定されている。本実施例の場合、多くのIPsec処理装置2が共通のポリシーを利用することで、配布ポリシー記憶部16に設定するポリシーの数を減らすことができる。

【0250】

ここで、n台のIPsec処理装置がすべての組合せで、互いにIPsecの

通信を実施する場合において、本実施例に必要な設定量と従来の I P s e c 处理装置に必要な設定量とを比較する。この時、すべての I P s e c 通信の組合せにおいて同一のポリシーを適用することとする。

【0251】

従来の I P s e c 处理装置に必要な設定量の合計は先に計算した通り、 $2^n (n - 1)$ である。それに対し、本実施例においては、 I P s e c 处理装置同士の通信の組合せの数に関わらず、 I P s e c ポリシーの設定量は 1 件だけでよい。したがって、本実施例において必要となる設定量は $4^n + 1$ となる。

【0252】

これからわかる通り、従来の手法では設定量が n の 2 乗に比例して多くなるが、本実施例では設定量が n に比例して大きくなるため、組合せが多くなるほど効果が大きくなることがわかる。例えば、 $n = 10$ の場合には、従来の手法の設定量が 180 に対して、本実施例の設定量が 41 となり、約 $1/4$ の設定で済むことがわかる。

【0253】

【発明の効果】

以上説明したように本発明の装置及び方法は、 I P s e c 处理装置間に適用する I P s e c のポリシーを一括管理することによって、通信する装置間での設定不一致を防止することができるという効果が得られる。

【0254】

また、本発明の他の装置及び方法は、要求メッセージを受信した場合に当該要求メッセージを送信した I P s e c 处理装置の通信相手である I P s e c 处理装置に対して当該通信用の要求メッセージを送信させるために要求起動メッセージを送信することによって、ポリシー設定後の暗号化や復号を滞りなく行うことができ、送信元からのパケットを取りこぼしなく受取ることができるという効果が得られる。

【0255】

さらに、本発明の別の装置及び方法は、 I P s e c の暗号化や認証に使用するための共有秘密鍵を生成し、その生成した共有秘密鍵を I P s e c 处理装置に配

布することによって、共有秘密鍵演算を不要とし、個々の装置での通信開始時の I P s e c 経路の接続時間を短縮することができ、性能の低下を防ぐことができるという効果が得られる。

【図面の簡単な説明】

【図 1】

本発明の一実施例による I P s e c によるネットワークの構成を示すブロック図である。

【図 2】

図 1 の I P s e c 設定サーバの構成を示すブロック図である。

【図 3】

図 2 の配布ポリシー記憶部の記憶内容を示す図である。

【図 4】

図 2 の管理テーブルの記憶内容を示す図である。

【図 5】

図 4 の S A パラメータの内容を示す図である。

【図 6】

本発明の一実施例による要求メッセージの一例を示す図である。

【図 7】

本発明の一実施例による配布メッセージの一例を示す図である。

【図 8】

本発明の一実施例による要求起動メッセージの一例を示す図である。

【図 9】

本発明の一実施例による該当なしエラーメッセージの一例を示す図である。

【図 10】

本発明の一実施例による内容不一致エラーメッセージの一例を示す図である。

【図 11】

本発明の一実施例による応答なしエラーメッセージの一例を示す図である。

【図 12】

本発明の一実施例による I P s e c 設定サーバの動作を示すフローチャートで

ある。

【図13】

本発明の一実施例によるIPsec設定サーバの動作を示すフローチャートである。

【図14】

図1のIPsec処理装置の構成を示すブロック図である。

【図15】

図14のSPDの内容を示す図である。

【図16】

図15に示すSPDの適用ポリシー(z)の一例を示す図である。

【図17】

図14のSADの内容を示す図である。

【図18】

図14のIPsec処理部の処理動作を示すフローチャートである。

【図19】

図14の設定管理部の処理動作を示すフローチャートである。

【図20】

図14の設定管理部の処理動作を示すフローチャートである。

【図21】

図2のSPDの内容の一例を示す図である。

【図22】

図21に示すSPDの適用ポリシー(v)の内容を示す図である。

【図23】

従来のIPsec処理装置のSPDの内容を示す図である。

【図24】

図23のSPDの適用ポリシー(j)の内容を示す図である。

【図25】

図2の管理テーブルのIPsec処理装置から要求メッセージを受信した後の内容を示す図である。

【図26】

図14のS P Dの配布メッセージを受信して適用ポリシーを設定した後の内容を示す図である。

【図27】

図2の管理テーブルのS Aを更新するために新しいエントリが生成される場合の内容を示す図である。

【図28】

本発明の一実施例によるI P s e c処理装置の動作を示すシーケンスチャートである。

【図29】

本発明の他の実施例によるI P s e c処理装置の構成を示すブロック図である。

【図30】

本発明の別の実施例による配布ポリシー記憶部の記憶内容を示す図である。

【図31】

従来のI P s e c処理装置の構成を示すブロック図である。

【図32】

従来のI P s e c処理装置の動作を示すシーケンスチャートである。

【図33】

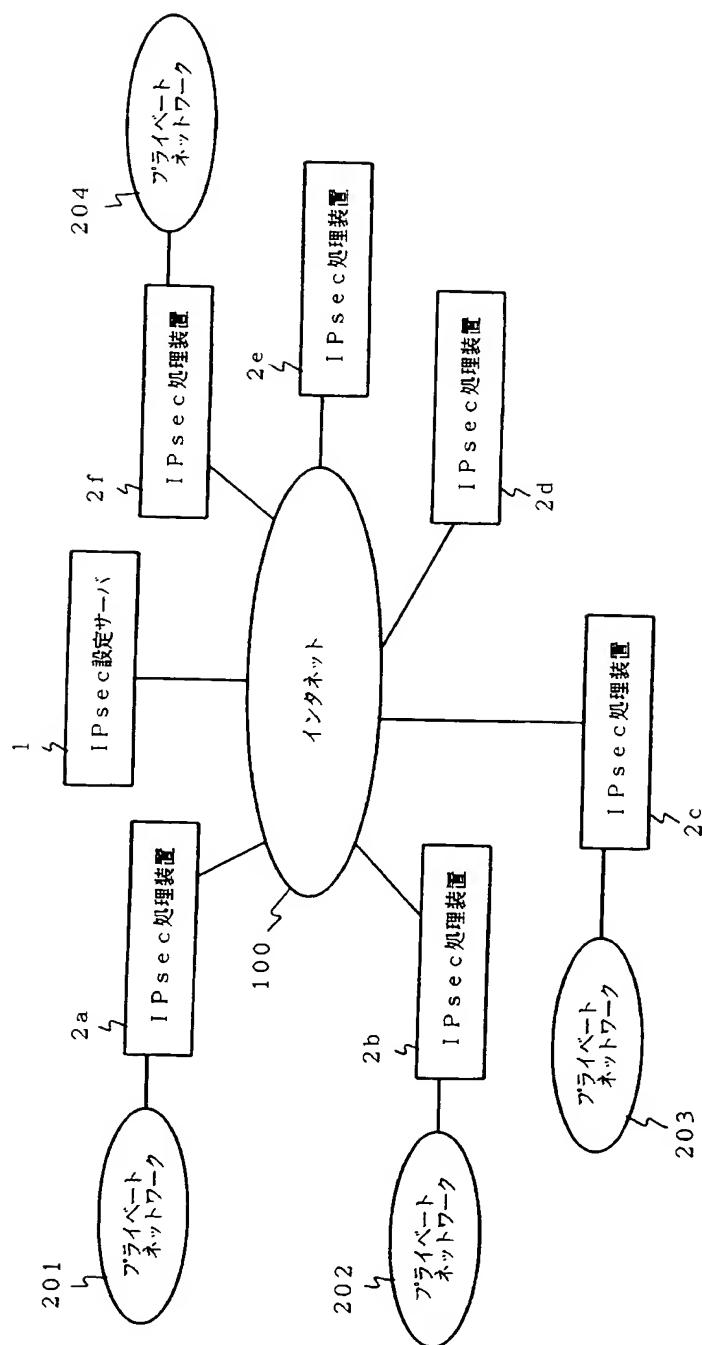
従来のI P s e c処理装置の他の構成を示すブロック図である。

【符号の説明】

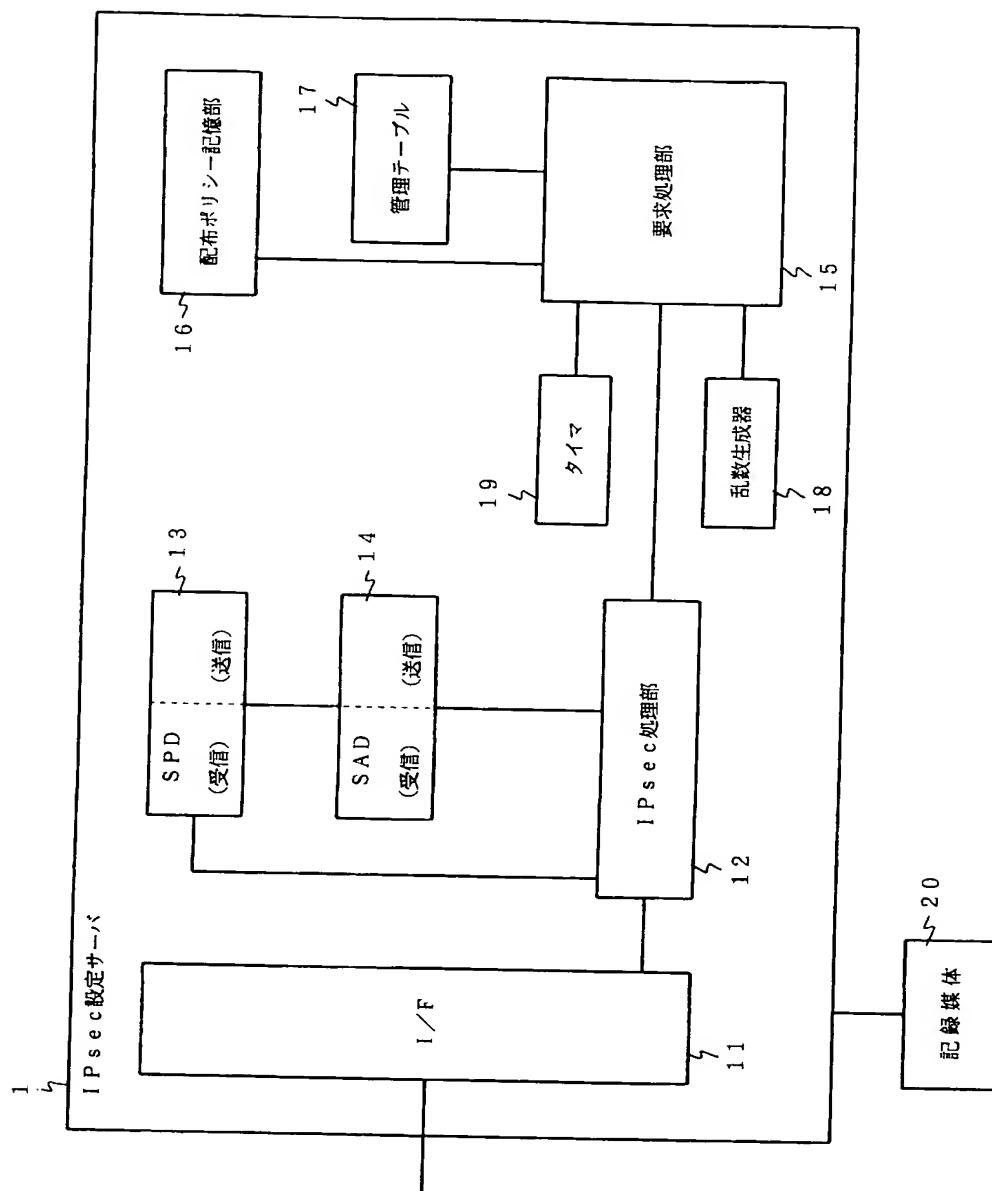
- 1 I P s e c 設定サーバ
- 2, 2 a ~ 2 f, 3 I P s e c 処理装置
- 1 1, 2 1, 2 2 インタフェース部
- 1 2, 2 3 I P s e c 処理部
- 1 3, 2 4 S P D
- 1 4, 2 5 S A D
- 1 5 要求処理部
- 1 6 配布ポリシー記憶部

- 17 管理テーブル
- 18 亂数生成器
- 19 タイマ
- 20, 28 記録媒体
- 26 設定管理部
- 27 ルーティング部
- 31 上位アプリケーション部
- 100 インタネット
- 201~204 プライベートネットワーク

【書類名】 図面
【図 1】



【図2】



【図 3】

アドレスペア	配布ポリシー
IPsec 處理装置 2 a	IPsec 處理装置 2 b IPsec プロトコル カブセル化モード 暗号化アルゴリズム 認証アルゴリズム SA の有効期間
IPsec 處理装置 2 d	IPsec 處理装置 2 e IPsec プロトコル カブセル化モード 暗号化アルゴリズム 認証アルゴリズム SA の有効期間

配布ポリシー (a)

配布ポリシー (b)

【図 4】

ID	要求元アドレス	相手先アドレス	要求ID	SPI	設定パラメータ
1	IPsec 処理装置 2a	IPsec 処理装置 2b	1001	5100	適用ポリシー 2a→2b用SAパラメータ 2b→2a用SAパラメータ 配布ポリシー (a) SAパラメータ (a) SAパラメータ (b)
	IPsec 処理装置 2b	IPsec 処理装置 2a	2001	6100	
2	IPsec 処理装置 2a	IPsec 処理装置 2b	1002	5110	適用ポリシー 2a→2b用SAパラメータ 2b→2a用SAパラメータ 配布ポリシー (a)
	IPsec 処理装置 2b	IPsec 処理装置 2a			
3					

【図5】

I P s e c プロトコル	E S P
カプセル化モード	トンネルモード
暗号化アルゴリズム	D E S - C B C
認証アルゴリズム	H M A C - M D 5 - 9 6
有効期限	3 6 0 0 秒
暗号化鍵	0 x 7 d 5 e 8 3 7 a d . . .
認証鍵	0 x 8 9 e 5 6 2 b f c . . .
I V	0 x c 3 2 f b e 0 0 4 . . .
受信側S P I	6 1 0 0

【図6】

メッセージタイプ	要求メッセージ
I D	1 0 0 1
要求元アドレス	I P s e c 処理装置 2 a
相手先アドレス	I P s e c 処理装置 2 b
S P I	5 1 0 0

【図 7】

メッセージタイプ	配布メッセージ
I D	1001
要求元アドレス	I P s e c 処理装置 2 a
相手先アドレス	I P s e c 処理装置 2 b
設定パラメータ	
運用ポリシー	配布ポリシー (a)
2 a→2 b用 SAパラメータ	SAパラメータ (a)
2 b→2 a用 SAパラメータ	SAパラメータ (b)

【図 8】

メッセージタイプ	要求起動メッセージ
相手先アドレス	I P s e c 処理装置 2 a

【図 9】

メッセージタイプ	該当なしエラーメッセージ
I D	1001
要求元アドレス	I P s e c 処理装置 2 a
相手先アドレス	I P s e c 処理装置 2 b

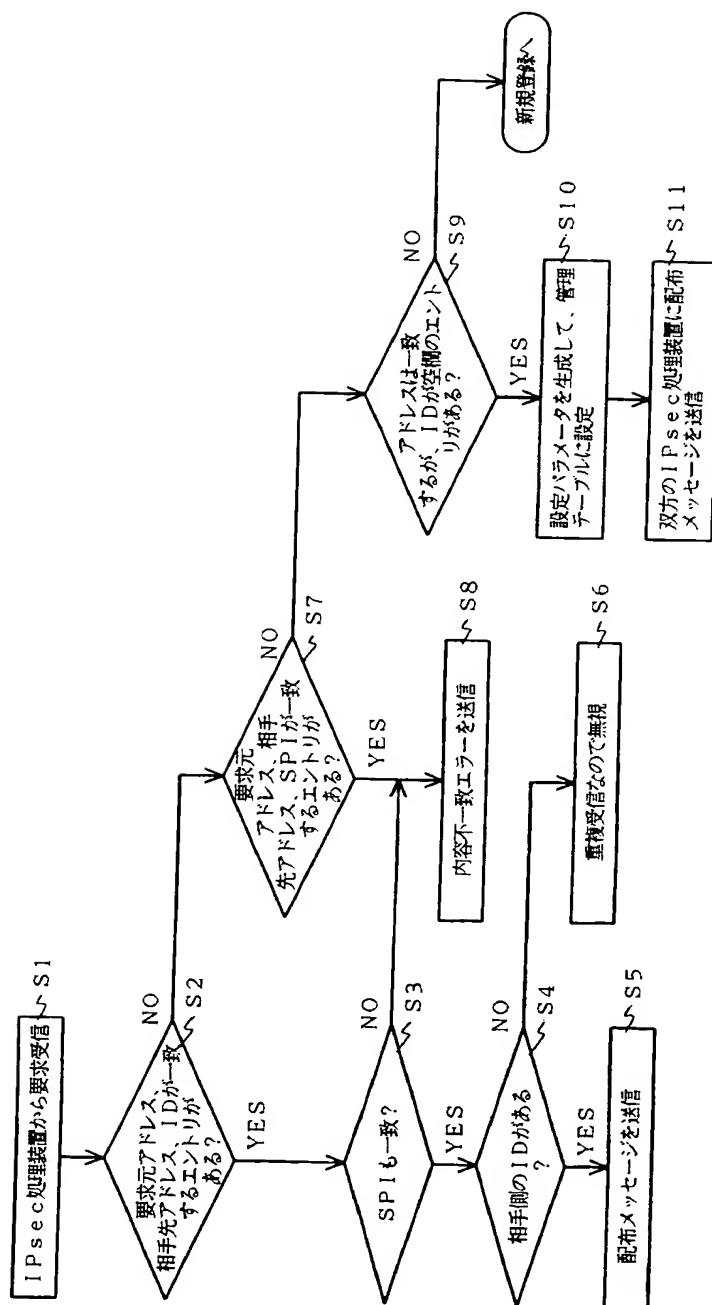
【図 10】

メッセージタイプ	内容不一致エラーメッセージ	
ID	1001	
要求元アドレス	IPsec処理装置2a	
相手先アドレス	IPsec処理装置2b	
エントリー一覧	ID	SPI
	1001	5100
	1002	5110

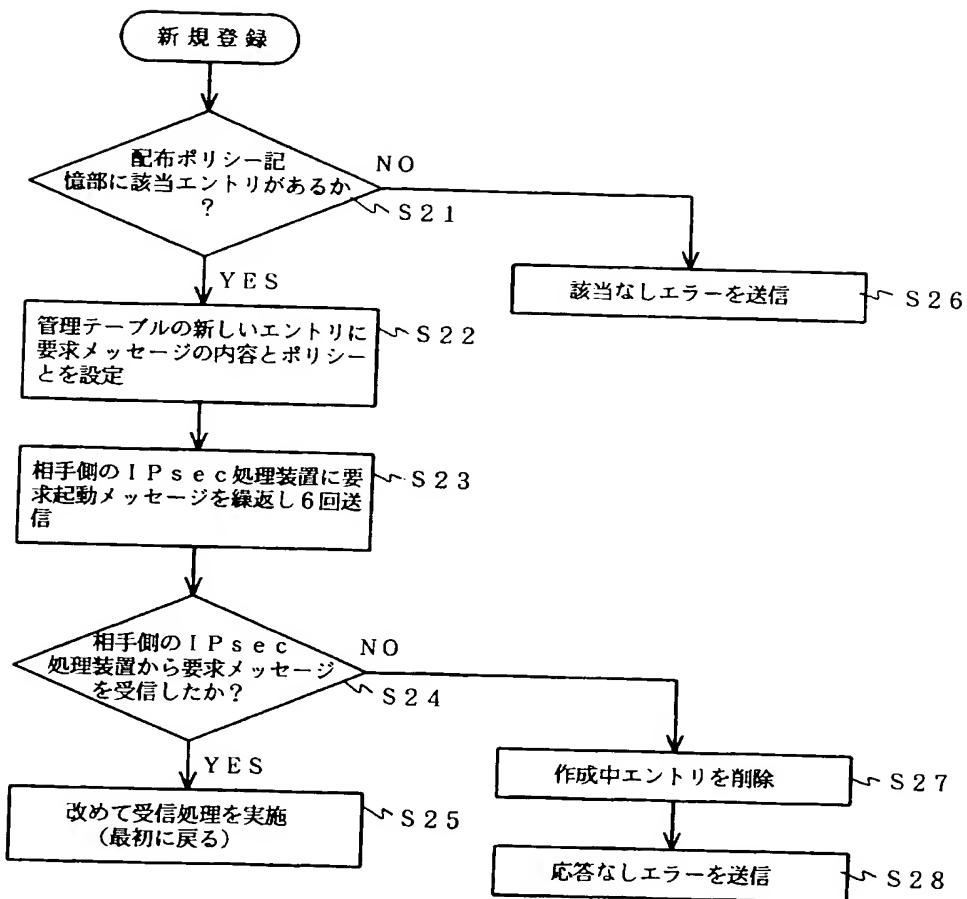
【図 11】

メッセージタイプ	応答なしエラーメッセージ
ID	1001
要求元アドレス	IPsec処理装置2a
相手先アドレス	IPsec処理装置2b

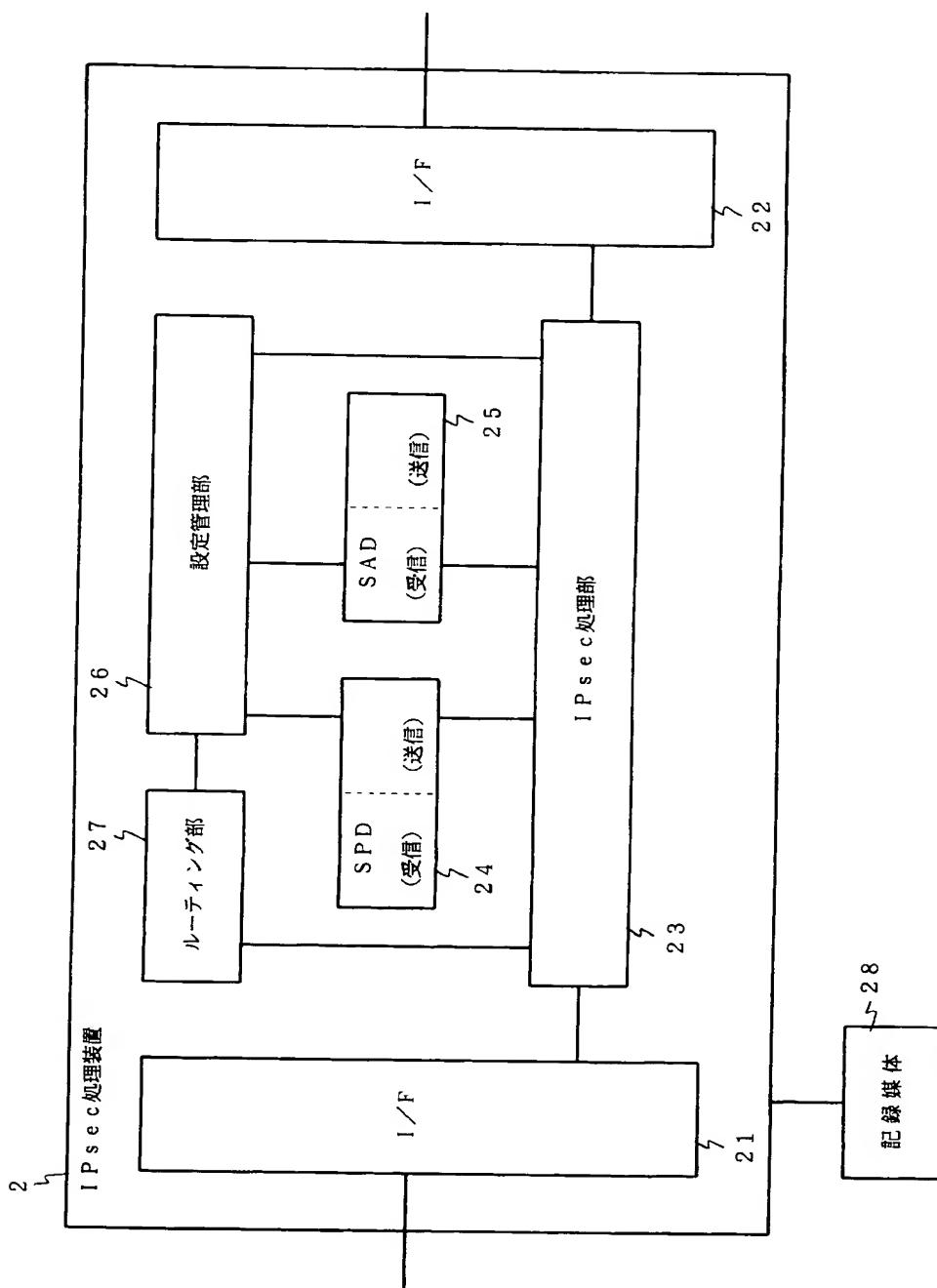
【図 12】



【図13】



【図 14】



【図 15】

ID	セレクタ	処理	IPsec 適用ポリシー	設定要求用相手アドレス
1	自分自身→設定サーバ1	IPsec	適用ポリシー(z)	
2	プライベート202宛	IPsec		IPsec処理装置2b
3	プライベート203宛	IPsec		IPsec処理装置2c
4	上記以外すべて	通過		

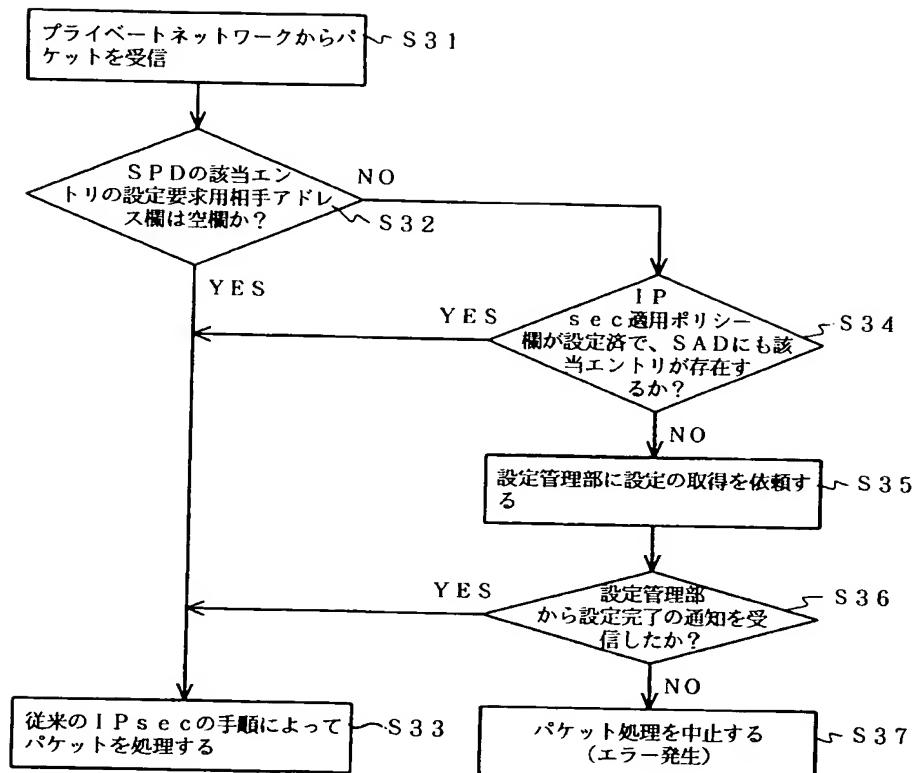
【図 16】

IPsec 適用ポリシー	
IPsec プロトコル	ESP
カプセル化モード	トランSPORTモード
相手先アドレス	設定サーバ1
暗号化アルゴリズム	AES-CBC
認証アルゴリズム	HMAC-SHA-1-96
SAの有効期間	3600秒
IKE ポリシー	
相手 IPsec 処理装置アドレス	設定サーバ1
相手認証方式	事前共有秘密鍵
事前共有秘密鍵	password-for-ike
暗号化アルゴリズム	DES-CBC
ハッシュアルゴリズム	MD5
Oakley グループ	1536ビットMODPグループ
SAの有効期間	3600秒

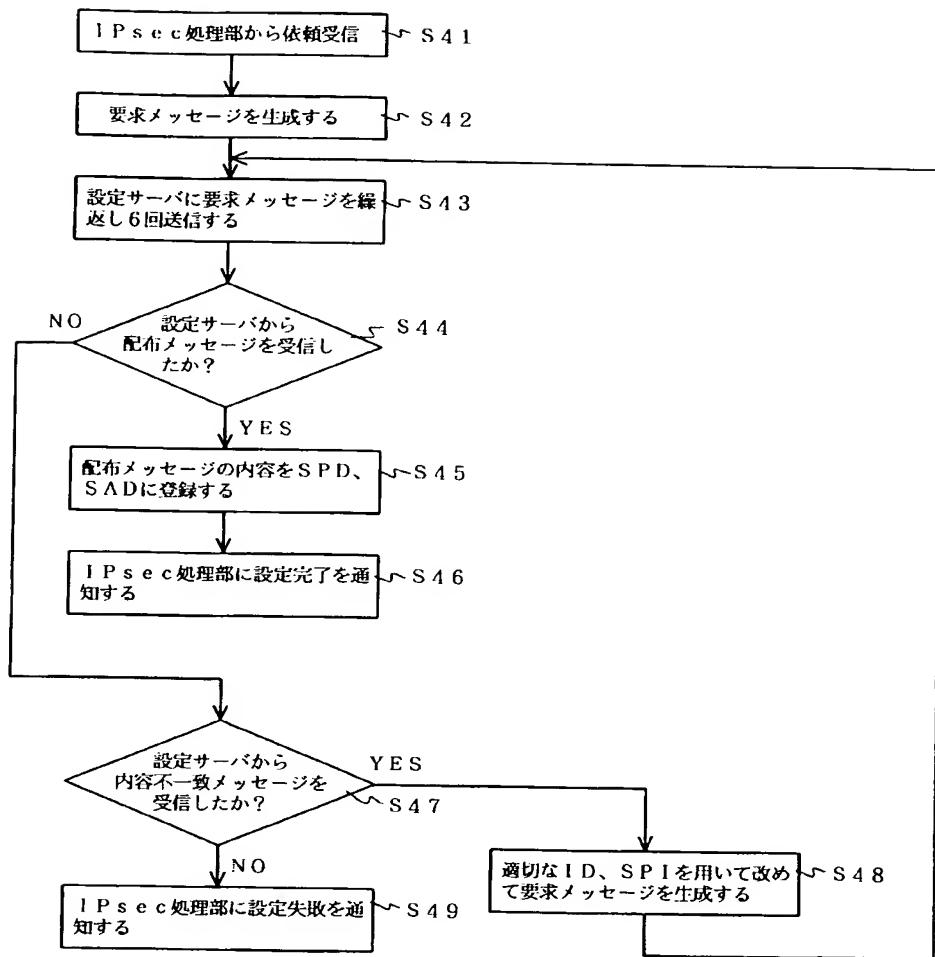
【図17】

ID	キー・パラメータ			SA・パラメータ
	終点アドレス	IPsec	ESP	
1	IPsec処理装置2b		ESP	6100 カプセル化モード 暗号化アルゴリズム 認証アルゴリズム 暗号化鍵 認証鍵 IV 有効期限 シーケンス番号
2	設定サーバ1		ESP	6100 カプセル化モード 暗号化アルゴリズム AES-CBC 認証アルゴリズム HMAC-SHA-1-96 暗号化鍵 認証鍵 IV 有効期限 シーケンス番号
3				

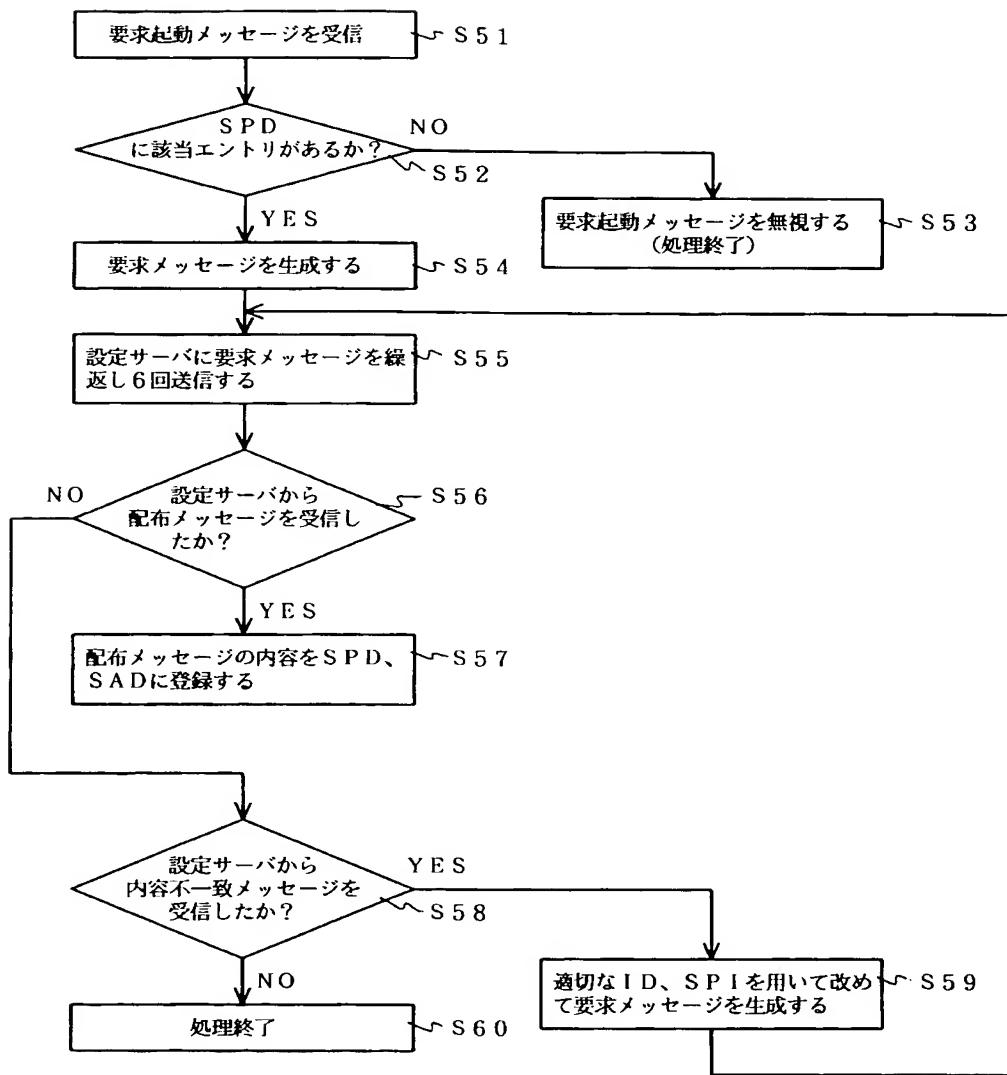
【図 18】



【図19】



【図20】



【図21】

ID	セレクタ	処理	IPsec適用ポリシー
1	IPsec設定サーバ1→IPsec処理装置2a	IPsec	適用ポリシー(v)
2	IPsec設定サーバ1→IPsec処理装置2b	IPsec	適用ポリシー(w)
3	IPsec設定サーバ1→IPsec処理装置2c	IPsec	適用ポリシー(x)
4	IPsec設定サーバ1→IPsec処理装置2d	IPsec	適用ポリシー(y)
5	上記以外すべて	廃棄	

【図22】

IPsec適用ポリシー	
IPsecプロトコル	ESP
カプセル化モード	トランSPORTモード
相手先アドレス	IPsec処理装置2a
暗号化アルゴリズム	AES-CBC
認証アルゴリズム	HMAC-SHA-1-96
SAの有効期間	3600秒
IKEポリシー	
相手IPsec処理装置アドレス	IPsec処理装置2a
相手認証方式	事前共有秘密鍵
事前共有秘密鍵	password-for-ike
暗号化アルゴリズム	DES-CBC
ハッシュアルゴリズム	MD5
Oakleyグループ	1536ビットMODPグループ
SAの有効期間	3600秒

【図23】

ID	セレクタ	処理	IPsec適用ポリシー
1	プライベート202宛	IPsec	適用ポリシー(j)
2	プライベート203宛	IPsec	適用ポリシー(k)
3	上記以外すべて	通過	

【図24】

IPsec適用ポリシー	
IPsecプロトコル	ESP
カプセル化モード	トンネルモード
相手先アドレス	IPsec処理装置2b
暗号化アルゴリズム	DES-CBC
認証アルゴリズム	HMAC-MD5-96
SAの有効期間	3600秒
IKEポリシー	
相手IPsec処理装置アドレス	IPsec処理装置2b
相手認証方式	事前共有秘密鍵
事前共有秘密鍵	password
暗号化アルゴリズム	DES-CBC
ハッシュアルゴリズム	MD5
Oakleyグループ	1536ビットMODPグループ
SAの有効期間	3600秒

【図25】

ID	要求元アドレス	相手先アドレス	要求ID	SPI	設定パラメータ
1	IPsec 処理装置2a	IPsec 処理装置2b	1001	5100	通用ポリシー 2a→2b用SAパラメータ 2b→2a用SAパラメータ
	IPsec 処理装置2b	IPsec 処理装置2a			通用ポリシー
2					
3					

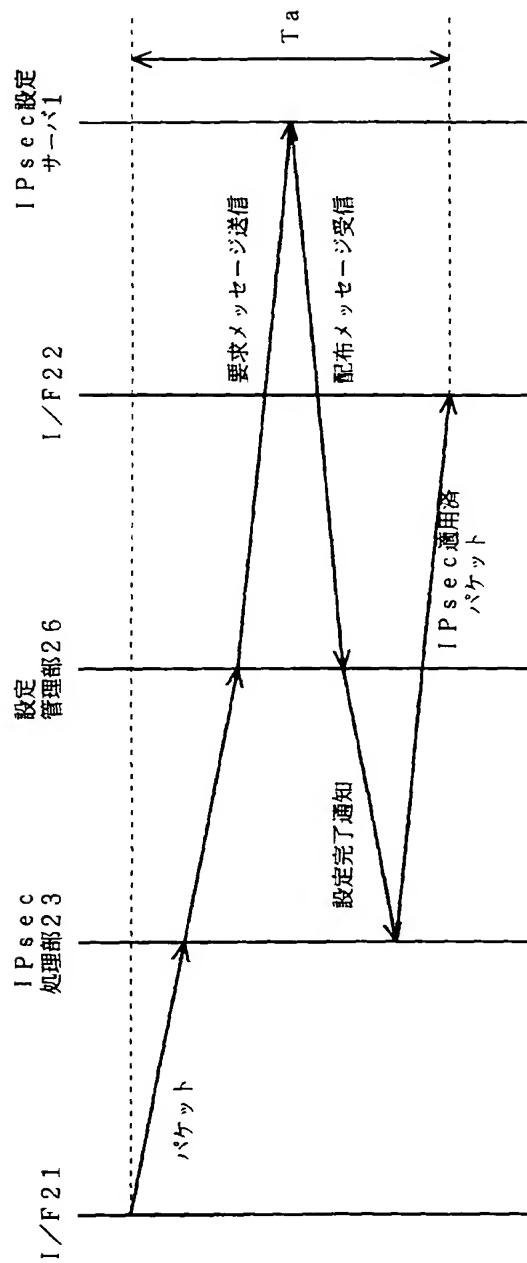
【図26】

ID	セレクタ	処理	IPsec適用ポリシー	設定要求用相手アドレス
1	自分自身→設定サーバ1	IPsec	適用ポリシー(z)	
2	プライベート202宛	IPsec	適用ポリシー(a)	IPsec処理装置2b
3	プライベート203宛	IPsec		IPsec処理装置2c
4	上記以外すべて	通過		

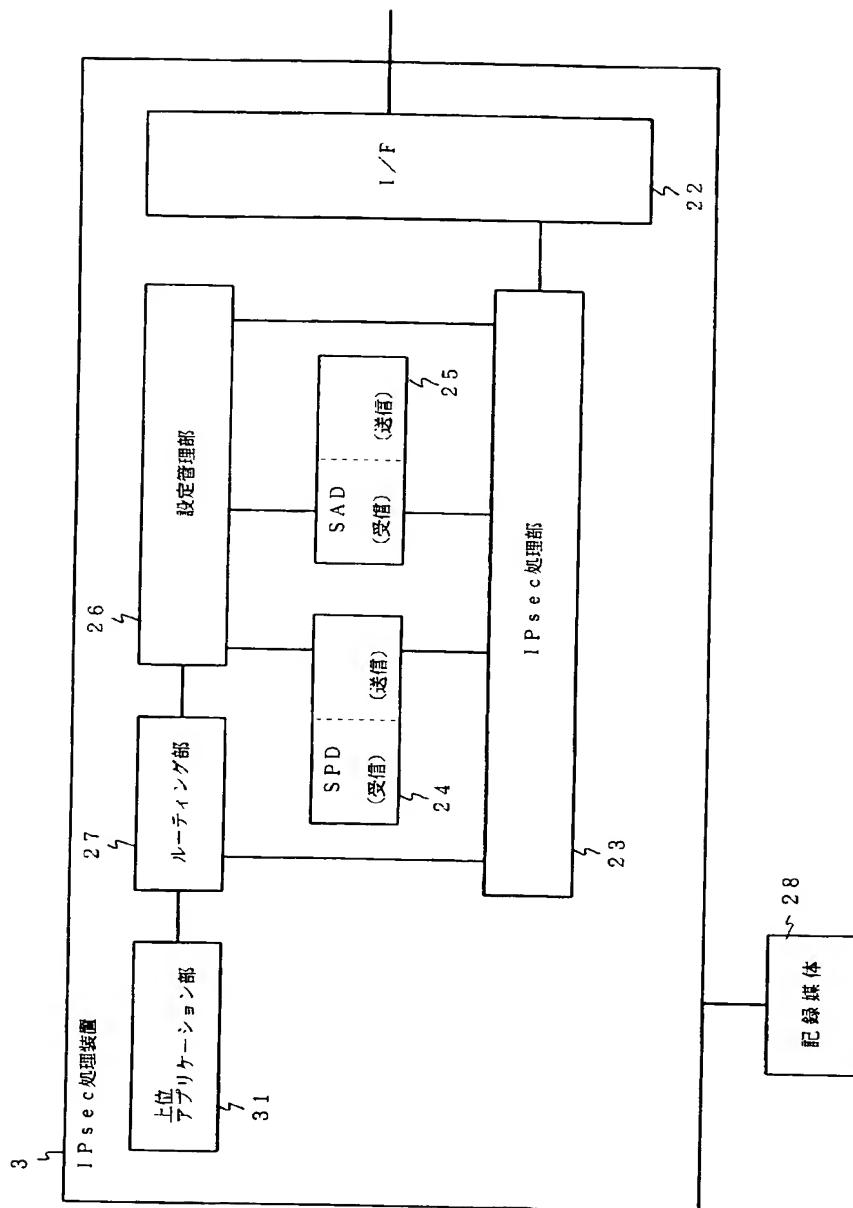
【図27】

ID	要求元アドレス	相手先アドレス	要求ID	SPI	設定パラメータ
1	IPsec 処理装置2a	IPsec 処理装置2b	1001	5100	適用ポリシー 2a→2b用SAパラメータ 2b→2a用SAパラメータ 配布ポリシー(a) SAパラメータ(a) SAパラメータ(b)
	IPsec 処理装置2b	IPsec 処理装置2a	2001	6100	
2	IPsec 処理装置2a	IPsec 処理装置2b	1002	5110	適用ポリシー 2a→2b用SAパラメータ 2b→2a用SAパラメータ 配布ポリシー(a) SAパラメータ(c) SAパラメータ(d)
	IPsec 処理装置2b	IPsec 処理装置2a	2002	6110	
3					

【図28】



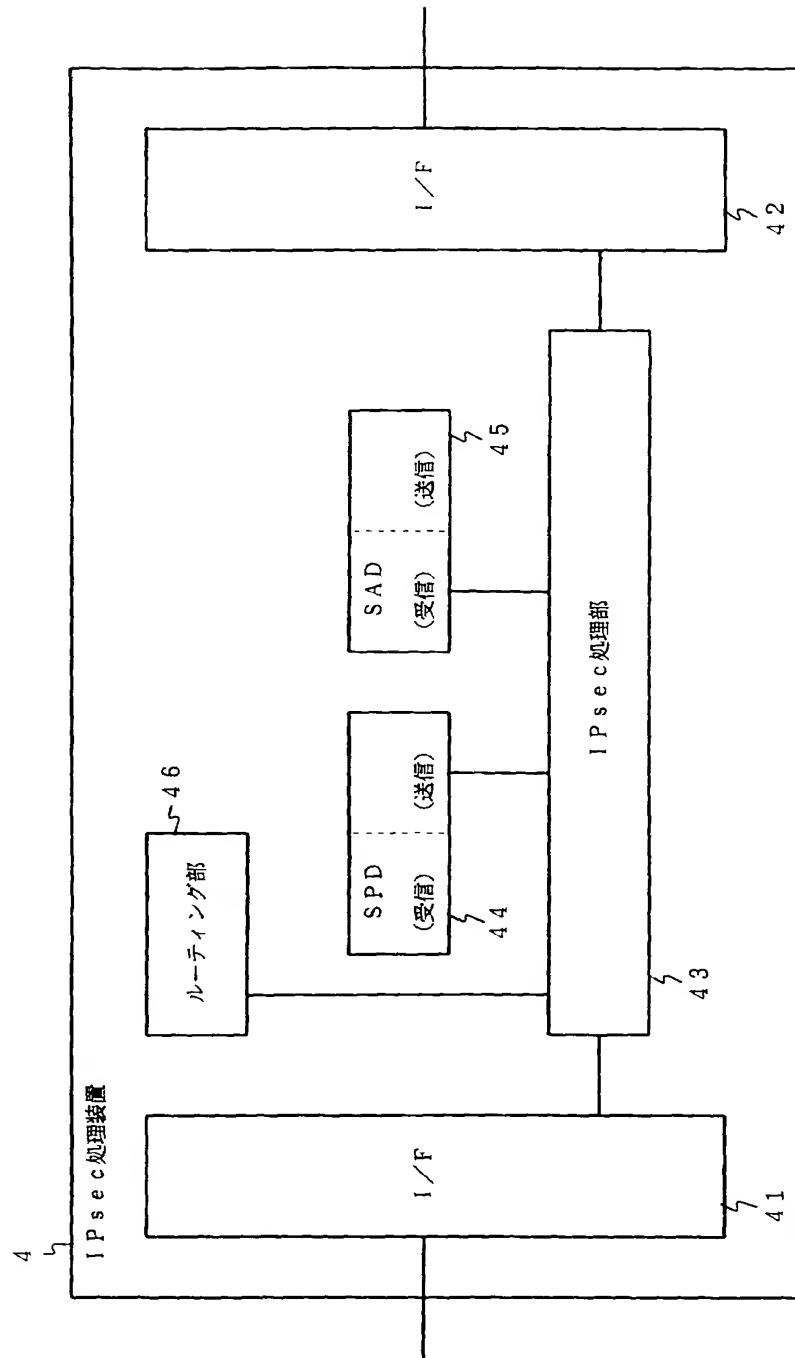
【図29】



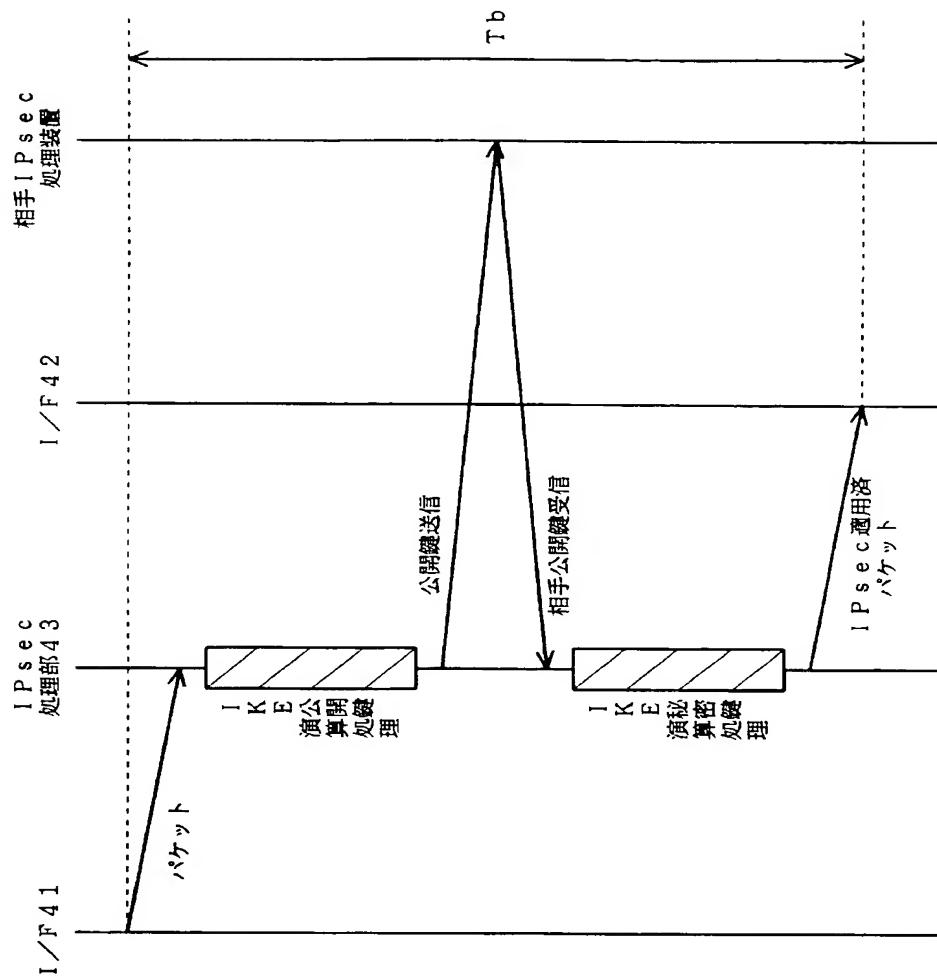
【図30】

アドレスペア	IPsec処理装置2d	IPsec処理装置2e	配布ポリシー
		IPsecプロトコル カブセル化モード 暗号化アルゴリズム 認証アルゴリズム SAの有効期間 3600秒	配布ポリシー (b) ESP トンネルモード 3DES-CBC HMAC-SHA-1-96
上記以外すべて		IPsecプロトコル カブセル化モード 暗号化アルゴリズム 認証アルゴリズム SAの有効期間 3600秒	配布ポリシー (a) ESP トンネルモード DES-CBC HMAC-MD5-96

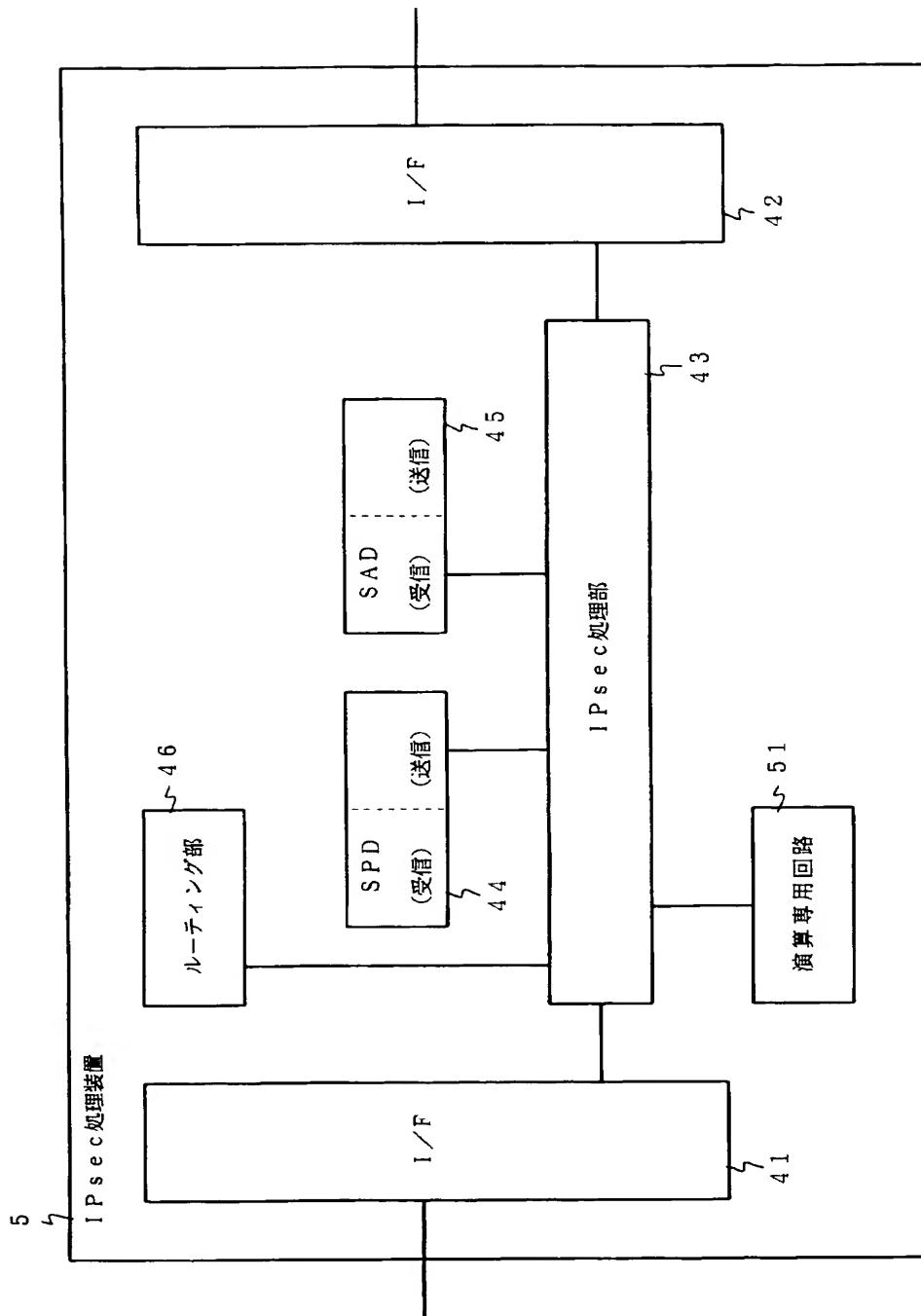
【図31】



【図32】



【図33】



【書類名】 要約書

【要約】

【課題】 通信する装置間での設定不一致を防止可能な I P s e c 設定サーバ装置を提供する。

【解決手段】 I P s e c 処理部 1 2 はインタフェース部 1 1 から受信したデータ通信パケットに対して I P s e c 処理を実施する。S P D 1 3 は I P s e c 処理部 1 2 から参照され、I P s e c を適用するためのポリシーを記録している。S A D 1 4 は I P s e c 処理部 1 2 から参照され、個々の通信に対して I P s e c 処理を実施するために必要な S A を記録している。要求処理部 1 5 は I P s e c 処理装置から設定要求メッセージを受信し、配布メッセージを返す。配布ポリシー記憶部 1 6 は要求された設定を決定するために必要な I P s e c ポリシーが記憶されている。管理テーブル 1 7 は設定要求を受けた各々の S A 通信に関する情報が記憶されている。

【選択図】 図 2

特願 2002-264913

出願人履歴情報

識別番号 [000004237]

1. 変更年月日 1990年 8月29日

[変更理由] 新規登録

住 所 東京都港区芝五丁目7番1号

氏 名 日本電気株式会社